MEMORIZABLE PUBLIC-KEY CRYPTOGRAPHY (MePKC) & ITS APPLICATIONS

Third draft (version 3.0)

LEE KOK WAH

DOCTOR OF PHILOSOPHY

MULTIMEDIA UNIVERSITY

APRIL 2011

MEMORIZABLE PUBLIC-KEY CRYPTOGRAPHY (MePKC) & ITS APPLICATIONS

BY

LEE KOK WAH

B.Eng.(Hons.) (Electrical Eng.), University of Malaya, Malaysia

M.Eng.Sc. (Computer Communications), Multimedia University, Malaysia

THESIS SUBMITTED IN FULFILMENT OF THE

REQUIREMENT FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

(by Research)

at the

Faculty of Engineering & Technology

MULTIMEDIA UNIVERSITY

MALAYSIA

April 2011

Copyright License of This Open-Source Book

DECLARATION

I hereby declare that the novel works have been done by myself and no portion of the work contained in this thesis has been submitted in support of any application for any other normal doctorate degree (i.e. Ph.D.) or qualification at this or any other university or institute of learning.

_____

LEE Kok Wah

ACKNOWLEDGEMENT

I hereby would like to express my gratitude to the following persons together with their inputs that have been given me in completing the electronic book of this PhD research project, which has contributed mainly in the novel knowledge field of key/password security leading to the memorizable public-key cryptography (MePKC) and its applications. Here are the listees:

(i) My parents, relatives and friends together with those anonymous people

- For help and giving me the physical, emotional and spiritual supports.

(ii) The nine investors, Malaysia

- For a total financial investment at about MYR$20,000 on the patent rights of DIP switch.

(iii) Lake-Tee Khaw, University of Malaya, Kuala Lumpur, Malaysia

- For giving the advantages and disadvantages of SD (Statutory Declaration).

(iv) Gita Radhakrishna, Multimedia University (MMU), Melaka, Malaysia

- For supplying the legal contents about copyright.

(v) Alan Wee-Chiat Tan, Multimedia University, Melaka, Malaysia

- For supplying C++ class of big number arithmetic after my given idea; and
- For being a nominal PhD supervisor since 16 August 2008 till 14 April 2009 and from 08 February 2010 till 20 March 2011.

(vi) Voon-Chet Koo, Multimedia University, Melaka, Malaysia

- For prototyping the RJ45 switch using conventional DIP switch on PCB.

(vii) Hong-Tat Ewe, Multimedia University, Cyberjaya, Malaysia

- For being a nominal PhD supervisor since 27 May 2004 till 15 August 2008; and
- For having lots of unpleasant and trust-less interactions.

(viii) Matt Bishop, University of California at Davis, CA, USA

- For supplying a proceedings paper.

(ix) Alex X. Liu, Michigan State University, MI, USA

- For supplying a journal paper.

(x) Chee-Onn Chow, University of Malaya, Kuala Lumpur, Malaysia

- For supplying a journal paper.

(xi) Ching-Weng Hong, Multimedia University, Melaka, Malaysia

- For conducting an experiment to look for the bounds of key strengthening.

(xii) Those three external thesis examiners

- For their criticisms to improve further the format and contents of this thesis.

(xiii) Vishnuvajjula Charan Prasad (Prof.), Multimedia University, Melaka, Malaysia

- For assisting to finalize the thesis format acceptable by MMU.

- For being a PhD supervisor since 21 March 2011 till 27 May 2011 or later.

DEDICATION

特将这本博士级研究论文献给于我敬爱的父亲李厚芳和母亲徐亚妹。

This normal doctorate thesis is dedicated to my respected and beloved parents, Hew-Fong Lee and Ah-Mooi Choi.

H-(^_^)-H

Find me Xpree or XpreeLi in the Internet!

^^^ Mottoes ^^^

Chinese: 语言与文字是了解一个文化的终极密钥。

Japanese: 言語(げんご)と文字(もじ)は文化(ぶんか)のかぎです。

English: Language and Writing are the ultimate keys to understand a culture.

Malay: Bahasa dan Tulisan adalah kunci-kunci terdasar untuk memahami satu ketamadunan.

ABSTRACT

This normal doctorate (i.e. Ph.D. degree in engineering) thesis proposes four main novel knowledge contribution components in the knowledge field of information security generally, and key management particularly. Kok-Wah Lee the author aims to realize the MePKC (Memorizable Public-Key Cryptography) by using fully mnemonic private key.

The prior arts of private key storage since year 1976 are encrypted private key, split private key, and roaming private key. Memorizability of secret key at a practical maximum key size at 100 bits has been an obstacle or open hard problem for about 30 years. A following problem is how to support a great number of needed passwords for important offline and online accounts.

Firstly, the author proposes 2D (Two-Dimensional) key input method and system to create high-entropy secret key. 2D key is in a 2D space to exceed the limits of single-line password field, due to its graphical nature to have mnemonic for easy memorizability, big key size till 256 bits, and high randomness to resist guessing attack and dictionary attack. Possible key styles of 2D key include multiline passphrase, crossword, ASCII art / Unicode art, colourful text, and sensitive input sequence.

Secondly, multihash key is proposed to have one master key from 2D key to generate multiple slave keys using key strengthening, hash truncation, and optional identity name (ID) or domain name (URL) for both the offline and online accounts. Those slave keys can fulfil the technical and legal demands of various cryptographic schemes to have different symmetric keys and asymmetric key pairs.

Thirdly, MePKC is proposed by using ECC (Elliptic Curve Cryptography) to use 2D key directly or indirectly via multihash key till 256-bit MePKC. Both 192-bit encryption scheme and signature scheme have been tested.

Lastly, anti-hacking data storage using improved DIP (Dual In-Line Package) switch is proposed to securely store original plaintext and decrypted ciphertext from virtual hacking over the computer communication network.

Figure 0.1a Multiline passphrase

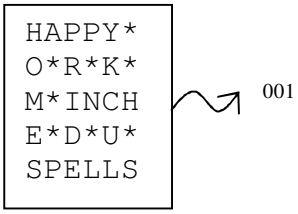


Figure 0.1b Crossword

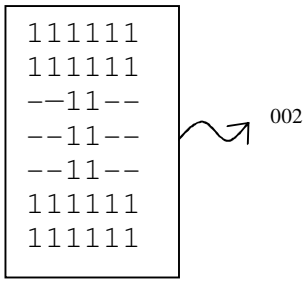


Figure 0.1c ASCII art

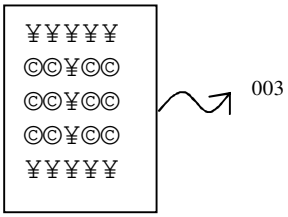


Figure 0.1d Unicode art

Figure 0.1 Two-dimensional (2D) key

Keywords: Key/password security, key management, big secret(s) creation methods, 2D key, multihash key, memorizable public-key cryptography (MePKC), anti-hacking data storage.

TABLE OF CONTENTS

COPYRIGHT PAGE ii

DECLARATION iii

ACKNOWLEDGEMENT iv

DEDICATION vi

ABSTRACT vii

TABLE OF CONTENTS ix

LIST OF TABLES xiii

LIST OF FIGURES xiv

PREFACE xv

CHAPTER 1: OVERVIEW 1

1.1 Introduction 1
1.2 Motivation 1
1.3 Research Aims 3
1.4 Research Methodology 4
1.5 Organisation of the Thesis 4

CHAPTER 2: LITERATURE REVIEW (PART 1): CONTEMPORARY MEMORIZABLE SECRET 7

2.1 Required Protection Periods and Their Key Sizes 7
2.2 Review of the Secret for Symmetric Key Cryptosystem 10
2.2.1 Related Work: Single-Line Key/Password Field 12
2.3 Review of the Secret for Asymmetric Key Cryptosystem 12
2.4 Potential Methods to Create Big and Yet Memorizable Secret 14

CHAPTER 3: LITERATURE REVIEW (PART 2): CREATING BIG MEMORIZABLE SECRETS 17

3.1 Passphrase Generation Methods 17
3.1.1 Acronym 17
3.1.2 Full Sentence 18

3.1.3 Diceware 18
3.1.4 Coinware 19
3.2 Other Matters about Creating Password 20
3.2.1 Environ Password 20
3.2.2 Password in Unicode Encoding 20
3.3 Related Work of 2D Key: Single-Line Key/Password Field 21
3.4 Key Strengthening 22
3.5 Memorizable Secret as a Master Key 23
3.5.1 Introduction 23
3.5.2 Related Works 26
3.6 Related Works of MePKC: Storages of Private Key 29
3.7 Related Prior Arts of Tools to Resist Hacking 30
3.8 Conclusion 31

CHAPTER 4: RESEARCH METHODOLOGY (PART 1): CREATING BIG MEMORIZABLE SECRET USING TWO-DIMENSIONAL (2D) KEY 32

4.1 Introduction 32
4.2 2D Key Input Method 34
4.3 Styles of 2D Key: Multiline Passphrase 37
4.4 Styles of 2D Key: Crossword 37
4.5 Styles of 2D Key: ASCII Art / Unicode Art 37
4.6 Styles of 2D Key: Colourful Text 39
4.7 Styles of 2D Key: Sensitive Input Sequence 39
4.8 Requirement of Key Size for 2D Key 39

CHAPTER 5: RESEARCH METHODOLOGY (PART 2): MULTIHASH KEY 41

5.1 Overview 41
5.2 Introduction 41
5.3 Basic Model of Multihash Key 42
5.4 Acceptable Time Bounds of Multihash Key 47

CHAPTER 6: RESEARCH METHODOLOGY (PART 3): APPLICATIONS OF BIG MEMORIZABLE SECRET & MePKC 48

6.1 Methods and Systems to Create Big Memorizable Secret 48
6.2 Potential Applications of Available Big Memorizable Secret 48
6.3 Main Applications for Symmetric and Asymmetric Key Cryptosystems 50
6.4 Prototyped Applications of Created Big Memorizable Secret(s) 51
6.5 Memorizable Symmetric Key to Resist Quantum Computer Attack 52
6.6 Memorizable Public-Key Cryptography (MePKC) 53
6.6.1 The Proposed MePKC Applications 6.4(ii)-(iii) 53
6.6.2 Selection of ECC Curve to Prototype MePKC Schemes 56

6.6.3 Encryption Scheme of MePKC 57
6.6.4 Signature Scheme of MePKC 59
6.7 Other Cryptographic, Information-Hiding, and Non-Cryptographic Applications of Secret beyond 128 bits 60

CHAPTER 7: RESEARCH METHODOLOGY (PART 4): ANTI-HACKING DATA STORAGE USING IMPROVED DIP SWITCH 62

7.1 Overview 62
7.2 Introduction 62
7.3 Proposing Improved DIP Switch 64
7.4 Method and Device to Secure Anti-Hacking Data Storage 66
7.5 Other Forms of Innovation 67

CHAPTER 8: RESULTS & DISCUSSIONS 69

8.1 Overview of Results 69
8.2 Two-Dimensional (2D) Key 69
8.2.1 Discussions: High-Entropy Secret 69
8.2.2 Limitations 70
8.2.3 Conclusion 70
8.3 Multihash Key 71
8.3.1 Discussions: Comparisons 71
8.3.2 Discussions: Suitable Time Bounds 71
8.3.3 Limitations 75
8.3.4 Conclusion 76
8.4 Memorizable Public-Key Cryptography (MePKC) 76
8.4.1 Discussions: Enablement of Amazing Functions 76
8.4.2 Limitations 79
8.4.3 Conclusion 79
8.5 Anti-Hacking Data Storage Using Improved DIP Switch 80
8.5.1 Discussions: Costs and Reliability 80
8.5.2 Limitations 82
8.5.3 Conclusion 83

CHAPTER 9: CONCLUSIONS 84

9.1 Concise Summary 84
9.2 Suggestions for Future Research 84
9.2.1 512-Bit Multihash Key Needs Hash Function beyond 1024 Bits 84
9.2.2 MePKC Extension to Other Non-Conventional Cryptographic Schemes 85
9.2.3 Big Secret(s) for Information-Hiding and Non-Cryptographic Applications 86
9.2.4 Safety Box Using Computerized Lock 86

9.2.5 Provable Security Studies 87
9.2.6 Statistical Surveys for Various Security Schemes 87
9.3 Future Development of Keys the Secret 87
9.4 Conclusions 89

APPENDIX A: WRITING SYSTEMS OF THE WORLD 90

APPENDIX B: CHILDREN-MADE 2D KEYS 93

APPENDIX C: CHRONOLOGY OF MY PhD STUDY 94

REFERENCES 97

ACRONYMS 122

PUBLICATION LIST BY K.-W. LEE 127

LIST OF TABLES

Table 2.1 Minimum symmetric key sizes for different security levels of protection 8

Table 2.2 Minimum asymmetric key sizes in equivalent with the security levels of symmetric key sizes 9

Table 2.3 Various key sizes corresponding to the numbers of ASCII characters and Unicode (version 5.0) characters 11

Table 3.1 Passphrase generation from acronym 17

Table 3.2 Minimum diceware words (7776 word list) for different security levels 19

Table 3.3 Conversions between binary and hexadecimal numeral systems 19

Table 3.4 Environ password 20

Table 4.1 Various key sizes corresponding to the numbers of ASCII characters, Unicode (version 5.0) characters, and settings sufficiency of 2D key input method 40

Table 5.1 Binary-to-text encoding Bin2Txt(H) of multihash key 45

Table 6.1 Dimensions of 2D key for various symmetric key sizes 50

Table 7.1 Operating modes of method and device to secure anti-hacking data storage 66

Table 8.1 Comparisons of key management tools 72

Table 8.2 One-second time bounds of several computer systems 74

Table A.1 Functional classification of writing systems 91

Table A.2 List of languages by number of native speakers 92

Table C.1 Development timeline of K. W. Lee's research project 94

LIST OF FIGURES

Figure 0.1 Two-dimensional (2D) key viii
Figure 4.1 Operation of 2D key input method and system 33
Figure 4.2 Pseudocode of 2D key input method and system 35
Figure 4.3 Styles of 2D key: Multiline passphrase 37
Figure 4.4 Styles of 2D key: Crossword 37
Figure 4.5 Styles of 2D key: ASCII art 38
Figure 4.6 Styles of 2D key: Unicode art 38
Figure 5.1 Pseudo-code to determine the numbers of hash iteration for multiple security levels of multihash key methods and systems 43
Figure 5.2 Operation of the basic model of multihash key method and system 44
Figure 5.3 Proposed usages of 20 security levels 46
Figure 6.1 Generations and applications of one/more big memorizable secrets 49
Figure 6.2 Operation of MePKC method and system 54
Figure 6.3 Encryption stage of MePKC encryption scheme (P-192) 58
Figure 6.4 Decryption stage of MePKC encryption scheme (P-192) 58
Figure 6.5 Signing stage of MePKC signature scheme (P-192) 59
Figure 6.6 Verification stage of MePKC signature scheme (P-192) 60
Figure 7.1 Structural diagram of conventional 10-way DIP switch 65
Figure 7.2 Structural diagram of proposed 10/12-way anti-hacking DIP switch 65
Figure 7.3 Innovated 10-way 8PST+2PST DIL switch activated in opposite direction 68
Figure 8.1 Overview of the four major novel knowledge contributions 69
Figure A.1 Writing systems of the world 90
Figure B.1 2D keys using ASCII art and Chinese characters meaning “twenty first day” [二十一日] 93
Figure B.2 2D keys using ASCII art and Chinese characters meaning “cloudy sky nurtures the woods” [云天工木] 93

PREFACE

This thesis is an output documentation of a research project applied on 12 November 2003 and registered on 27 May 2004 to achieve three aims at one stroke. These three aims are to solve an imperative research problem, to develop intellectual properties (IPs) to support an entrepreneurship, and to qualify a person for a doctoral degree.

The proposal defence seminar, first work completion seminar, second work completion seminar, notice of thesis submission request, and MMU (Multimedia University) approval of this thesis title to enable its experts' evaluation are on 14 March 2005, 18 February 2008, 2 July 2008, 23 July 2008, and 1 December 2008, respectively. Nevertheless, this thesis is mainly prepared in October 2008.

Upon the author's decision for not furthering his doctoral research studies under the Lee Foundation Scholarship as communicated by Professor Michael T.-C. Fang due to a sudden author's family constraint, this research project began with its idea conception in the end of 2003 by having the official PhD project application date on 12 November 2003. It began with the studies of multimedia communications security in general and autosophy communications in particular. Then, in October 2005, some novel ideas were conceptualized on how to protect the data crystal of autosophy communications in particular, which was then generalized for any common computer data protection, to networked information security, and any applications of big secret beyond 128 bits in information engineering. Here, for these idea series conceptualized since October 2005 and applied for MMU financing as investment to protect the IP (Intellectual Property) rights like patent, MMU refused to finance the patent protection but utility model of partial idea series, and gave up the patent rights on 25 September 2007 and 29 August 2008.

Let's create and maintain a networked info-computer age for a more paperless, trip-less, petroleum-less, and environment-friendly human society by having safer multipartite electronic computer communications as from the original and novel knowledge contribution of this research project.

The copyright of this thesis is a print edition as a remix and derivative from an earlier online electronic publication (Lee, 2009a) in the Internet for public peer review. I hereby notify that the novel work have all been done by myself and no portion of the work contained in this thesis, except Appendix B to have some new and creative child-made ASCII arts by Wei-Tong Chui and Wei-Jian Chui.

Kok-Wah LEE @ Xpree Jinhua Li (李国华 @ 李锦华)
Find me Xpree or Xpreeli in the Internet!
Email: E96LKW@hotmail.com (Home); contact@xpreeli.com (Business)
URL: www.xpreeli.com/homepage/kwlee.htm (Home); www.xpreeli.com (Business)
First unpublished draft (06 April 2009)
Second unpublished draft (17 March 2010)
Third unpublished draft (30 April 2009)

CHAPTER 1 OVERVIEW

1.1 Introduction

The world human population in April 2010 has achieved beyond 6.9 billion. At the same time, the world climate, resources, and environment are having red alarms on. Information communications technologies (ICT), especially the electronic communications of Internet, are believed to be tools to reduce the paper usages and transportation demands, as well as to cultivate a global economy with smoother demands and supplies. Security, health, food and beverages, accommodation, family, career, education, finance, sex, entertainment, sport, etc. are human major concerned topics. Their importance is in descending order for a majority of people.

Here, when ICT is applied to preserve more Earth resources and to conserve friendly environment, information security is always a major people concern for important computer communications. As for the Internet, identity theft is a serious crime in the electronic commerce and electronic government. Yet another serious offence is copyright piracy of literary works, software, music, image, and video. Due to the hacked computer databases of human records, the rights of privacy and publicity are also hard to be controlled and guarded.

1.2 Motivation

In term of information security, it mainly consists of cryptology, information hiding, and random number generator (RNG). Cryptology further consists of cryptography and cryptanalysis. Information hiding further consists of steganography and digital watermarking. RNG further consists of hardware RNG and software pseudo-random number generator (PRNG).

To access and control a user identity of an information security system, there are four types of authentication factors: What you know like secret, what you have like token, what you are like biometrics (Menezes, Oorschot, & Vanstone, 1996; Boatwright & Luo, 2007), and whom you know like introducer (Brainard, Juels, Rivest, Szydlo, & Yung, 2006), in the ascending order of implementation costs.

These factors can be used individually or mixed. Among them, password the secret is the most prevailing one for applying the symmetric key cryptography in the Internet due to the low implementation costs, as well as good hardware and software compatibilities. However, a secret, especially a long one, is subject to the forgetfulness or the exposure of a secret written down. The situation becomes worse when there are lots of accounts to be handled. If a secret is used for multiple accounts, there exists domino effect of password reuse problem (Ives, Walsh, & Schneider, 2004). Moreover, the memorizability size of a secret using the current prior art is limited to 128 bits for a protection period of 30 years. To solve these problems, token or biometrics, optionally together with a bi-factor using another secret, is used.

Nevertheless, token has the weaknesses of poor hardware and software compatibilities, low portability when number of tokens per user is many, high implementation costs due to installation and maintenance, easy loss, possible dropping damages, and token cracking (de Koning Gans, Hoepman, & Garcia 2008; de Winter, 2008; Garcia, de Koning Gans, Muijrers, van Rossum, Verdult, Schreur, & Jacobs, 2008).

Meanwhile biometrics has the disadvantages of poor hardware and software compatibilities, domino effect due to limited biometrics to support multiple accounts, no perfect accurate system due to FAR (False Acceptance Rate) and FRR (False Rejection Rate), low usability and efficiency due to no universal accessibility and no permanent availability from physiological and medical factors (Maghiros, Punie, Delaitre, Lignos, Rodríguez, Ulbrich, Cabrera, Clements, Beslay, & van Bavel, 2005) like plastic surgery, high implementation costs due to installation and maintenance, as well as irreplaceability and irreusability problems of biometrics upon hacking and stealth.

For examples of no universal accessibility of biometrics authentication systems, there is no support for homozygotic twins, 5% of human are not fingerprint recognition supported (Haylock, No date; Maltoni, Maio, Jain, & Prabhakar, 2003; Vacca, 2007, p. 280) due to diseases like eczema (“Singaporean Female,” 2008) and arthritis, human undergone surgery changing the facial structure needs re-enrolment for face recognition, 1.8 aniridia patients out of 100,000 births and patients after laser

iridotomy to correct angle-closure caused by glaucoma have no iris and are not iris recognition supported, eyes alignment problem with camera of blind people and patients of pronounced nystagmus (tremor of the eyes) are poorly iris recognition supported, wheelchair users have usability problems of camera location and insufficient height variation, cataract patients after operation may need re-enrolment, and today DNA methods fail to differentiate monozygotic twins. For example of no permanent availability, the high biometrics deformation rates of very young and very old require frequent re-enrolment.

For the fourth authentication factor of "whom you know" like introducer and referee, even though the authentication burden of the introducee can be relieved, the burden has in fact been transferred to the introducer and it is up to the introducer to use the authentication factor of what you know, what you have, and/or what you are. Furthermore, there exist trust, responsibility, and obligation problems between the introducer and introducee. The human interaction models (Kurokawa, 1988, 1990, 1991, 1997) are then required to analyze the security probability of this factor.

In view of the limitations of token and biometrics, how good if the weaknesses of secret like memorizability and entropy size can be improved until the token and biometrics are not needed for majority applications.

1.3 Research Aims

Here, the first main focus of this research project is for this direction: Methods and systems to create big and yet memorizable secret(s). From a sufficiently large and yet memorizable master key, it shall be possible to derive multiple unique slave keys for multiple offline and online accounts. These slave keys shall be impossible to be used to derive other slave keys.

For public-key cryptography (PKC), the smallest practically secure private key size is 160 bits by using the FFC (Finite Field Cryptography) or ECC (Elliptic Curve Cryptography) (Gehrmann & Näslund, 2005, 2006, 2007; E. Barker, W. Barker, Burr, Polk, & Smid, 2007a, 2007b). Using the current prior arts like encrypted private key, split private key (Ganesan, 1996b), and roaming private key (Baltzley, 2000), there has been no fully memorizable private key yet.

Here, the second main focus of this research project is to develop fully memorizable private key towards MePKC (Memorizable Public-Key Cryptography), aka MoPKC (Mobile Public-Key Cryptography). The third research focus is to securely store the original plaintext and decrypted ciphertext of the first and second foci for various cryptographic applications in the field of information engineering.

1.4 Research Methodology

This research project originally contributes novel methods and systems to create big and yet memorizable secret(s), and then MePKC for various applications in information engineering. As from Spafford (1993), there are three types of techniques to prove a model in a computing dissertation: Analytic method using formal manipulations, stochastic method using statistical measurements, and building a prototype for experimental testing.

For the research methodology of this research project, the third method of building a prototype is used to show that it is possible to create big and yet memorizable secret by using 2-dimensional (2D) key (Lee, 2006a, 2008i, 2009c, 2010a), and further for the practical realization of MePKC (Lee & Tan, 2006; Lee, 2008j).

For security strength and protection period of various security schemes in this research project, the first method of analytically formal manipulations is needed, where Kok-Wah Lee the author has mainly adopted other researchers' analytic and experimental results. Since the author cum researcher is an electrical engineer and not educated as a mathematician, the reduction-based security (aka provable security) approach is only tried on his best effort as time allows. Hence, those cryptographers from the mathematics field are expected to carry out some provable security studies on the security schemes proposed here, whenever the big secret creation method(s) is applied, especially for the MePKC and its applications.

1.5 Organisation of the Thesis

Generally, the present invention of this thesis relates to computer communications security. Particularly, the present invention relates to key management of cryptography and information security. Most particularly, the present invention relates to methods and systems to create big and yet memorizable secrets that are large enough for the higher levels of security strength of security systems like AES-256, 256-bit ECC, 256-bit PRNG, and so on, (where AES stands for Advanced Encryption Standard; ECC stands for Elliptic Curve Cryptography; and PRNG stands for Pseudo-Random Number Generator), together with their derived applications in the general field of information engineering and specific field of information security like memorizable public-key cryptography (MePKC).

Specifically, the present invention broadly provides novel generation method and system of big memorizable secrets to practically realize stronger security levels of cryptographic, information-hiding, and non-cryptographic applications in the information engineering, especially MePKC (Memorizable Public-Key Cryptography).

The first independent embodiment of the present invention is the method and system to create big and yet memorizable secrets. The second independent invention embodiment is mutlihash key using hash iteration and hash truncation to create multiple slave keys from a single master key. From these two independent inventions, there are then various types of dependent inventions for various practical applications mainly due to the existence of big memorizable secrets, especially the important MePKC as the third main novel contribution of this doctorate study. For the fourth main novel contribution, Kok-Wah Lee the inventor has proposed an anti-hacking data storage using improved DIP (Dual In-Line Package, aka DIL) switch to securely keeping the original plaintext and decrypted ciphertext.

The organisation of this thesis has three components: Preliminary section, chapter section, and postscript section. The preliminary section consists of front page, copyright page, declaration, acknowledgements, dedication, abstract, table of contents, list of tables, list of figures, and prefaces. For the postscript section, it has appendices to show the writing systems of the world, children-made 2D keys, and

chronology of my PhD study; references; acronyms; and a publication list by K.-W. Lee.

There are nine chapters in the chapter section. Chapter 1 is an overview of this research project. Chapters 2 and 3 present the literature review in two parts. Chapters 4 to 7 are the main body to propose all the four main novel knowledge contributions done by Kok-Wah Lee, where they are 2D key, multihash key, MePKC and its applications, and anti-hacking data storage using improved DIP switch, respectively. Chapter 8 presents the results and discussions on four of the main novelty claims. Chapter 9 is the conclusions of this thesis by giving a concise summary on the originally contributed novel knowledge and some suggestions for future research.

In details, Chapter 4 proposes a big memorizable secret creation method called 2D (two-dimensional) key by entering key styles like multiline passphrase, crossword, ASCII art / Unicode art, colourful text, sensitive input sequence, etc., into a matrix-like 2D space.

Chapter 5 presents a method and system called multihash key to generate multiple unique slave keys (aka site keys) from a master key for both offline and online accounts. This multihash key uses hash iteration and hash truncation. Every slave key is computationally infeasible to be used to derive another slave key. The multihash key is integrated with 2D key for various applications of big secrets.

Chapter 6 tells the influential applications of big secrets from the integration of 2D key and multihash key. The most important one will be the MePKC, like its encryption scheme and signature scheme.

Chapter 7 is a hardware contribution to further secure the computer communications of MePKC from virtual hacking over a connected computer communications network like Internet. It is about an anti-hacking data storage using improved DIP switch.

CHAPTER 2 LITERATURE REVIEW (PART 1): CONTEMPORARY MEMORIZABLE SECRET

2.1 Required Protection Periods and Their Key Sizes

According to Kerckhoffs' law (Schneier, 1996), a cryptosystem shall depend 100% on the secrecy of password or key only. In the words of Shannon's maxim, it means "enemy knows the system". This law makes the civilian cryptosystem to have publicly known algorithm except the classified governmental and military information. This is needed to gain the public confidence for general daily applications from the fear of possible backdoor. There are various applications of secret in information engineering. Here, the required protection periods and their key sizes are briefly discussed to know how big a memorizable secret shall be.

If a cryptographic algorithm is securely tested, the required key length in character (L_C) of a password will depend on the factors of number of characters (C), key space (S), secure period (T), guesses per unit of time (G), and probability of guessing (P) (U.S. Department of Defense, 1985). The minimum key length has to be able to resist the brute force attack. The relationships of L_C, C, S, T, G and P are given in Equations (2.1) and (2.2).

$$S = \frac{GT}{P} \tag{2.1}$$

$$L_C \geq \left\lceil \frac{\log_2 S}{\log_2 C} \right\rceil \tag{2.2}$$

Nowadays, character encoding of ASCII is the most popular computing code. ASCII has some key sets of 26 lowercase characters, 26 uppercase characters, 10 digits, 62 alphanumeric characters, 33 non-alphanumeric characters, 95 printable characters, etc. If a key only has symbols of digits, its specialized name is *passcode*. If a key is long or consists of printable characters, it is named as *passphrase*.

There were once three Data Encryption Standard (DES) challenges as in year 1997, 1998, and 1999. Using the distributed network computing, maximum guesses of 2.45×10^9 keys per second was once recorded. For the latest guesses per computer

as at end of year 2005, it was about $1.5x10^7$ keys per second. The increment rate follows the Moore's Law, where computer performance is doubled for every 18 months. This indicates that strong password has to be longer as time passing by if there is no special key processing added.

Key length in bit (L) means that there are 2^n possible keys for n-bit key. By year 2010, the required key is 80 bits for symmetric key algorithm as announced by U.S. National Institute for Standards and Technology (NIST). Meanwhile, asymmetric key algorithm, like RSA, needs 1024 bits to be equivalently strong with 80-bit symmetric key algorithm as claimed by RSA Security. The key space varies and depends on the security requirements.

For the AES suggested by NIST to replace the DES, it has three types of symmetric key sizes. These key sizes are 128, 192, and 256 bits. Therefore, we have AES-128, AES-192, and AES-256 to fulfill the demands of security levels at 128, 192, and 256 bits (E. Barker, W. Barker, Burr, Polk, & Smid, 2007a, 2007b). For other security levels at 80 and 112 bits, NIST suggested two-key Triple Data Encryption Algorithm (2TDEA) and three-key Triple Data Encryption Algorithm (3TDEA), respectively (E. Barker, W. Barker, Burr, Polk, & Smid, 2007a, 2007b).

Table 2.1 Minimum symmetric key sizes for different security levels of protection

Key Size, bit		Protection
# 1	32	Individual attacks in "real-time". Only acceptable for authentication tag size.
# 2	64	Very short term protection. Obsolete for confidentiality in new systems.
# 3	72	Short to medium term of protection depending on organization size.
# 4	80	Smallest general purpose level, < 5 years protection.
# 5	112	Medium term protection. About 20 years.
# 6	128	Long term protection. Good, generic application independent recommendation, about 30 years.
# 7	256	Foreseeable future. Good protection against quantum computers.

Password choice depends on the strength and memorizability. Strength depends on key size in bit. Memorizability depends on number of memorized secrets in a human brain. For minimum key sizes at different security levels, it is shown in Table 2.1 (Gehrmann & Näslund, 2005, 2006, 2007).

For short term memory of English-based digit, Miller (1956) showed an average of 7 items plus or minus 2 (7 ± 2) (Jones, 2002). The good option is longer key size in bit and still memorizable. Some articles on memory can be referred (Baddeley, Thomson, & Buchanan, 1975; Ellis & Hennelly, 1980; Hoosain & Salili, 1988; Cowan, 2001) and we can see that a user has 6.5 unique passwords in average (Florencio & Herley, 2007), or 4 to 5 unrelated keys (Adams & Sasse, 1999). These are textual secret; whereas graphical secret has higher memorizability (Standing, Conezio, & Haber, 1970; Standing, 1973).

On the other hand, there are 3 conventional mathematical hard problems used in asymmetric key cryptosystem, which is also called public-key cryptosystem. These problems are integer factorization problem, discrete logarithm problem, and elliptic curve discrete logarithm problem. NIST categorizes the applications of these problems for public-key cryptography as integer factorization cryptography (IFC), finite field cryptography (FFC), and elliptic curve cryptography (ECC), respectively.

IFC has a long key size for public and private keys. FFC has a long public key and a short private key. ECC has a short key size for public key and private key. The minimum asymmetric key sizes for IFC, FFC, and ECC in equivalent with the security levels of symmetric key sizes are shown in Table 2.2 (E. Barker, W. Barker, Burr, Polk, & Smid, 2007a, 2007b).

Table 2.2 Minimum asymmetric key sizes in equivalent with the security levels of symmetric key sizes

Security (bits)	IFC		FFC		ECC	
	Public	Private	Public	Private	Public	Private
80	1024	1024	1024	160	160	160
112	2048	2048	2048	224	224	224
128	3072	3072	3072	256	256	256
192	7680	7680	7680	384	384	384
256	15360	15360	15360	512	512	512

A good password has to be strong and memorizable (Gehringer, 2002). The random password with printable ASCII characters is the strongest password but it is

poor in memorizability (Yan, Blackwell, Anderson, & Grant, 2004). However, password with good memorizability tends to be weak password and under the password cracking threats of guessing and dictionary attack (Klein, 1990). As time lapses, longer key length is needed due to the advancement of computer technology. Hence, the trend is the strong and memorizable passphrase or special key processing technique like key strengthening is adopted to get rid of the quest of longer key size.

The most popular email encryption software called Pretty Good Privacy (PGP) 9.0 (PGP Corporation, 2006) allows a maximum of 255 characters to be the passphrase. Microsoft Windows operating systems also have this feature. Methods exist on how to create secure keys (Adams, Sasse, & Lunt, 1997; Brown, Bracken, Zoccoli, & Douglas, 2004). Thus, a research problem is here asking on how to have big enough and yet memorizable secret(s) for various applications in information engineering, generally, and information security engineering, particularly.

2.2 Review of the Secret for Symmetric Key Cryptosystem

In civilian information security, according to Kerckhoffs' law, a security system shall depend fully on the secrecy of a key, and not the algorithmic software nor its hardware. The main reason for this law is that public confidence has to be earned to show that there is no backdoor in the security system relying solely on the secrecy of key, and disclosing its algorithm and hardware to the public, especially academic and corporate researchers, for comments.

For authentication to a security system, it basically has four methods: Secret for what you know, token for what you have, biometrics for what you own, and person for whom you know. Due to the factors of cost, hardware and software compatibilities, password/key the secret is the most popular. Short key is called password and long key is called passphrase. The key selection is always the balance of the factors of memorizability and security. Long and random key is securer but harder to remember. The current prior art of single-line key input field limits the practical memorizable key size to a maximum of 128 bits for majority normal users.

To create longer password called passphrase, there are now four existing methods: Sentence-type passphrase, acronym-type passphrase, diceware, and

coinware. Sentence-type passphrase is memorizable and has long key size, but vulnerable to dictionary attack; whereas acronym-type passphrase taking the first, last, other locations, or hybrid location is memorizable and resists to dictionary attack, but has a small key size. Diceware and coinware use several dices and coins, respectively, to randomly select a word from monolingual, bilingual, or multilingual wordlists, where they can resist dictionary attack, but memorizability reduces as the key size becomes longer. Hence, these passphrase generation methods are still insufficient to create random, memorizable, and yet big secret, that can resist guessing attack and dictionary attack, to fulfil the need for secret bigger than 128 bits.

Table 2.3 Various key sizes corresponding to the numbers of ASCII characters and Unicode (version 5.0) characters

Key size (bit)	80	96	112	128	160	192	256	384	512
Number of ASCII character (6.57 bits)	13	15	18	20	25	30	39	59	78
Number of Unicode character (16.59 bits)	5	6	7	8	10	12	16	24	31

According to Bruce Schneier (2006, 2007), for a survey of 34,000 MySpace users' passwords, about 99% of the passwords had 12 ASCII characters or less. An ASCII character carries about 6.57 bits, which means 99% of the 34,000 MySpace passwords had 78.84 bits or less. This reflected the facts that almost all the symmetric keys of the current symmetric key cryptosystems in practice reached at a key size less than 128 bits. In other words, memorizable key the secret is only practically applicable to the current popular symmetric key cryptosystems like 112-bit 3TDES (3-Key Triple Data Encryption Standard) and 128-bit AES (Advanced Encryption Standard). However, in a large-scale password habit survey (Florencio & Herley, 2007), the average password size is about 40.54 bits, most key size is rare to be more than 100 bits, and a user has 6.5 passwords for 25 accounts where 8 accounts in average are used daily.

Table 2.3 shows the numbers of ASCII and Unicode (version 5.0) characters for various key sizes. In Unicode 5.0, there are 98,884 graphic symbols or 16.59 bits per graphic symbol. The repertoire of Unicode graphic symbols can be upgraded

from time to time in future versions to enlarge the number of graphic symbols. Memorizable keys for 192-bit and 256-bit AES are out of the reach of the current key management method and system. Hence, need exists to have better key management method and system to create larger key/password the secret larger than 128 bits.

2.2.1 Related Work: Single-Line Key/Password Field

Conventionally, when secret is used for authentication, single-line key field will be the area for a user to enter a key. For the current longest possible key, it is a single-line passphrase. Passphrase can be formed from acronym, sentence, diceware, and coinware (Lee & Ewe, 2006). Nevertheless, limit exists due to the problems of memorizability and ASCII character input from keyboard. The first problem is due to the human factor; whereas the second is due to the user interface. These problems prohibit the applications of symmetric key sizes at higher security levels, whenever a user cannot remember and/or conveniently enter a long single-line passphrase.

2.3 Review of the Secret for Asymmetric Key Cryptosystem

Besides the symmetric key cryptography, asymmetric key cryptography or public-key cryptography (PKC) is one of the two main components in the field of cryptography. PKC emerged in the 1970s (Diffie & Hellman, 1976; Goldwasser, 1997). Symmetric key cryptosystem has a shared secret key between a pair of users, but each PKC user has an asymmetric key pair consisting of a private key known only to the user and a public key shared with the other users. Amazingly, PKC can solve the key sharing and distribution problems of symmetric key cryptosystem. Moreover, PKC can resist the guessing attack, dictionary attack, and pre-computation attack that symmetric key cryptosystem is susceptible to. Nevertheless, PKC processing speed is about 1000 times slower than the symmetric key cryptography. Consequently, PKC and symmetric key cryptosystem have to be used in hybrid mode for maximum performance of effectiveness.

Now, there are three main conventional asymmetric cryptosystems: IFC (Integer Factorization Cryptography), FFC (Finite Field Cryptography), and ECC

(Elliptic Curve Cryptography). IFC is based on the mathematical hard problem of integer factorization. FFC is based on discrete logarithm problem. And ECC is based on elliptic curve discrete logarithm problem.

RSA (Rivest-Shamir-Adleman) cryptosystem is a type of IFC being the very first practical realization of PKC since 1977. FFC like ElGamal encryption and DSA (Digital Signature Algorithm), as well as ECC were firstly introduced in the 1980s. Then, there are other PKC based on different mathematical hard problems but not yet well-standardized. Nevertheless, so far all the key sizes of asymmetric private key for IFC, FFC and ECC are too big to be human-memorizable. The large key sizes of RSA cryptosystem for its both private and public keys, as well as FFC cryptosystem for its public key, have even caused the USA government to shift to ECC having significantly smaller public and private key sizes. For more details on their practically secure key sizes, please refer to two NIST articles (E. Barker, W. Barker, Burr, Polk, & Smid, 2007a, 2007b).

Due to the reason that private key is not fully human-memorizable using the current prior art, a private key is either fully or partially in the form of a token. In the mean time among the prior art, there are three basic methods for private key storage: (i) Encrypted private key stored in the local computing system or device; (ii) split private key firstly proposed by Ravi Ganesan (1996b) on 18 July 1994 in the US Patent US5,557,678; and (iii) roaming private key firstly proposed by Cliff A. Baltzley (2000) on 25 November 1998 in the US Patent US6,154,543. All the three methods are bi-factor or multi-factor authentication, where at least one factor is a secret and another factor is a software token or hardware token.

The first method of private key storage encrypts the private key using a symmetric key and stores ciphertext of private key in the local computing system like hard disk drive or a device like smartcard, floppy disk, or USB flash drive. Encrypted private key method suffers from the problems of loss, damage, side-channel attacks, mobility, hardware and software compatibility, and password domino cracking effect of its digital certificate carrying only one asymmetric public key.

The second method splits a private key into two or more portions, where the first portion is a memorizable password or derivable from the memorizable password

kept by the owner of that private key. The second and possibly other portions of the private key are kept by one or more servers in the encrypted form like the first method. The first, second and possibly other split portions of the private key may also be derived from various authentication factors like token and biometrics. Split private key method suffers from the problems of malicious central authority attack on the user's short password, dictionary attack on the stolen encrypted partial private key, and password domino cracking effect of its digital certificate carrying only one asymmetric public key.

For the third method, roaming private key also has encrypted private key but its ciphertext is stored in a network system like server, and owner of the private key can download it from anywhere and anytime as long as the user has network access. The roaming private key method suffers from the problems of side-channel attacks, hardware and software compatibility, malicious central authority, dictionary attack on the stolen encrypted private key, and password domino cracking effect of its digital certificate carrying only one asymmetric public key.

In the US Patent US7,113,594, Boneh and Franklin (2006) described a new type of PKC called identity-based cryptography (IDC). In this method, a user's unique public identity like email or phone number is the public key and hence memorizable. However, its private key is not memorizable and has to be generated by a trusted third party (TTP).

Notwithstanding, as compared with symmetric key cryptosystem using password or key the secret, the popularity of token-based PKC using fully or partially encrypted private key, is low due to the problems of mobility convenience, implementation costs, hardware and software compatibilities, and management difficulty of certificate revocation list. Hence, there exists a need to get rid of fully or partially encrypted private key, and to invent key input method to let the private key fully human-memorizable as like the symmetric key.

2.4 Potential Methods to Create Big and Yet Memorizable Secret

One of the many invented methods here to create big and yet memorizable secret is to innovate the graphical password or picture password. From psychological

studies, it claims that human graphical memory is stronger than human textual memory. The graphical password is categorized into recognition-based and recall-based methods by Xiaoyuan Suo, Ying Zhu, and G. Scott Owen (2005). For recognition-based method, it can be the types of cognometrics and locimetrics. Meanwhile for recalled-based method, it can be the type of drawmetrics.

Passfaces invented by J. H. E. Davies (1997), as in the US Patent US5,608,387, is a type of cognometircs, where a user is requested to recognize some pre-selected image sequence of human faces as password. Davies' method has the weakness of low entropy per image. For G. Blonder's method (1996), as in the US Patent US5,559,961, it is a type of locimetrics, where a user has to select a few areas of an image in sequence as password. Blonder's method is vulnerable to hot-spot attack and shoulder-surfing attack. For Draw-a-Secret scheme by I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin (1999), it is a type of drawmetrics, where a user draw lines and points on a grid in the form as like a hidden hand signature. For this Draw-a-Secret scheme, its weakness is its authentication process for either acceptance or rejection is not exact as in the previous two graphical password methods, but estimation having FAR (False Acceptance Rate) and FRR (False Rejection Rate).

Besides these three main groups of graphical password, there are icon-like graphical password scheme by P. V. Haperen (1997), as in the UK Patent Application GB2,313,460, and event-based graphical password scheme by J. Schneider (2004), as in the US Patent Application US2004/0250138. The both of these latter methods are cognometric. Their common weakness is that the key space or password space is limited by the fine differentiation capability of human visual memory over images that may have only minor differences. This causes the entropy per image selection to be still unsatisfactory not big enough for the demands of information engineering for the stronger security levels to carry more bits of strength. Hence, need exists to boost the key space of graphical password for higher entropy per image selection, and yet still human-memorizable and visually differentiable.

Another potential method to have big memorizable secret is to create Chinese language password (CLPW) through Chinese character encodings and their

Romanization. T. D. Huang (1985), as in the US Patent US4,500,872, proposed on 19 February 1985 to use phonetic encoding and symbolic encoding to represent a Chinese character. The character space of Chinese language is huge by more than 16 bits per character and yet human-memorizable and differentiable. This CLPW method can also be extended to other CJKV languages due to the common sharing for the usages of Han characters (漢字 or 汉字) like Chinese Hanzi, Japanese Kanji, Korean Hanja, and Vietnamese Hán Tự. However, the current CLPW has a weakness that it is subject to dictionary attack. Hence, there exists a need to create CLPW resisting the dictionary attack.

There are some inventions to create password that can resist the dictionary attacks. Among them are (i) "System and Method for Generating Unique Passwords" by Martin Abadi, Krishna Bharat, and Johannes Marais (2000) in the US Patent US6,141,760; (ii) "Password Generation Method and System" by M. R. McCulligh (2003) in the US Patent US6,643,784; (iii) "Method and System for Automated Password Generation" by P. M. Goal and S. J. Kriese (2004) in the US Patent Application US2004/0168068; (iv) "Method and Apparatus for Password Generation" by M. R. Dharmarajan (2005) in the US Patent Application US2005/0132203; and (v) "Method and System for Generating Passwords" by B. E. Moseley (2006) in the US Patent Application US2006/0026439. Nevertheless, even though these five methods can resist dictionary attacks, they have lower memorizability. Hence, there exists a need not only to have a password generation method that can resist dictionary attack, but can have high memorizability as well even for a big secret at least and beyond 128 bits.

Yet another method to create a memorizable secret bigger than the current prior art was proposed by Whitfield Diffie and William A. Woods (2006) in their patent application filed on 22 June 2006 entitled "Method for Generating Mnemonic Random Passcodes", US Patent Application US2007/0300076. However, the password created by this method is not yet big enough for many applications in the information engineering.

CHAPTER 3 LITERATURE REVIEW (PART 2): CREATING BIG MEMORIZABLE SECRETS

3.1 Passphrase Generation Methods

Civilian cryptosystem applies Kerckhoffs' law to have security dependency 100% on the password secrecy. This reflects the fact that key length and key space are very important to ensure enough entropy or randomness to secure a cryptosystem. For stronger password, passphrase is suggested. Currently, there are three methods to generate passphrase: Acronym, full sentence and diceware. Moreover, an alternate method to diceware is proposed by Kok-Wah Lee the author: Coinware (Lee & Ewe, 2006), by using the coin. This method is not included in detailed in this thesis but only brief introduction. For more information, please refer to the published article.

Table 3.1 Passphrase generation from acronym

Sentence	Passphrase
Passwords should be impossible to remember and never written down	psbitranwd
Passwords should be impossible to remember and never written down	PsBiTrAnWd
Good or bad, you have to do it.	Goby,htdi.
Good or bad, you have to do it.	Drd,ueoot.
It may be a few sentences. One, two or more.	Imbafs.O,tom.

3.1.1 Acronym

For the passphrase created using the acronym (Schneier, 1996; PGP Corporation, 2006; Yan, Blackwell, Anderson, & Grant, 2004), a user has to remember one or a few sentences. Then, the first, second, or last, etc. characters of each word in the sentence(s) are joined to form an acronym. Both alphanumeric and non-alphanumeric ASCII characters may become the character of the acronym. The techniques of *capitalization* and *permutation* may be used to increase the randomness. This acronym will then act as the key. It has the features of high randomness and short key length. The examples of this method are shown in Table 3.1.

3.1.2 Full Sentence

The passphrase generation using the acronym is sufficient if the key length requirement is short. When the minimum key size demand is long, normally one full sentence or a few short sentences are entered directly as the key (Schneier, 1996; PGP Corporation, 2006; Yan, Blackwell, Anderson, & Grant, 2004). So far, it is an open problem to type the entire phrase into a computer with the echo turned off (Schneier, 1996). If the masked password is shown during the password entering process, then it will subject to shoulder surfing attack.

Besides, since the passphrase of full sentence has each word to be selected associatively, its randomness is magnitude-wise high but relatively low if password ciphertext is available. For example, super-user of any computing system can easily obtain ciphertext of the password. By gaining access to the encrypted password, the threats of ciphertext-only attack and frequency analysis of short cryptogram (Hart, 1994; Lee, Teh, & Tan, 2006) are then possible. For instance, the unicity distance of English language is about 30 characters. Once the encrypted password is equal to or more than the unicity distance, unique decipherability of the encrypted password will be feasible.

3.1.3 Diceware

Using full sentence for passphrase generation, the word frequency distribution can be under computational analysis (Kučera & Francis, 1967). To get rid of the association of words, diceware (PGP Corporation, 1996) introduced by A. G. Reinhold is an improved passphrase generation method.

There are many software pseudo-random number generators (PRNGs). Unfortunately, they have lots of pitfalls (Eastlake, Crocker, & Schiller, 1994) to ease any possible attack. Hence, some hardware random number generators (RNGs) such as coin and dice are very much better than the software PRNGs.

Diceware uses dice to select a word from an ordered word list. The word list can be in any language and based on senary or base-6 numeral system. For the most popular diceware, it is an English word list with 7,776 (= 6^5) words. Five dice values

are needed to locate one word randomly. Every selected word carries entropy of 12.92 bits. Table 3.2 shows the minimum diceware words for different security levels.

Table 3.2 Minimum diceware words (7776 word list) for different security levels

Key Size (bit)		32	64	72	80	112	128	256
Diceware	word	3	5	6	7	9	10	20
	bit	38	64	77	90	116	129	258

3.1.4 Coinware

In addition to diceware using dice, we have *coinware* using coin as proposed by (Lee & Ewe, 2006). Coin tossing is conducted to generate random passphrase. Each face of the coin is labelled as binary bits "0" and "1", respectively. Four coin values are used to derive a hexadecimal digit. Therefore, the word list is in hexadecimal order. Table 3.3 shows the conversions between the binary (BIN) and hexadecimal (HEX) numeral systems.

Table 3.3 Conversions between binary and hexadecimal numeral systems

BIN	HEX	BIN	HEX	BIN	HEX	BIN	HEX
0000	0	0100	4	1000	8	1100	C
0001	1	0101	5	1001	9	1101	D
0010	2	0110	6	1010	A	1110	E
0011	3	0111	7	1011	B	1111	F

Coinware uses four coins to create one hexadecimal digit. The created word lists are in hexadecimal order and can be applied for multilingual passphrase generation. Its exemplary application for Chinese language password is very useful. Readily-made Chinese character word list in the Unicode CJK unified ideographs enables fast hexadecimal reading for random passphrase generation. Hanyu Pinyin and Sijiao Haoma are used to Romanize and uniquely represent each Han character. Meanwhile, Jyutping and Rōmaji are used for Cantonese and Japanese languages, respectively.

3.2 Other Matters about Creating Password

3.2.1 Environ Password

An analogue to the Romanization of Chinese language to have alphabets and digits is the Environ password (Anderson, 2001, p. 49). Good memorizability exists when it is linked to a learnt language. For English language, U.K. government introduced the case insensitive Environ password in October 2005 for short-term protection. It has an 8-character key pattern as in Table 3.4. This pronounceable password has 34.9 bits per unit.

Table 3.4 Environ password

Form	[consonant - vowel - consonant - consonant - vowel - consonant - digit - digit] [consonant - vowel - consonant – digit - consonant - vowel - consonant - digit]
Example	pinray34, yankan77, supjey56, kinkin99; pin3ray4, yan7kan7, sup5jey6, kin9kin9

3.2.2 Password in Unicode Encoding

Unicode unifies the Han characters of CJK languages into CJK unified ideographs or Unihan under ISO 10646. There are three major blocks of Han characters or Chinese characters in the Unicode character encoding: CJK unified ideographs, CJK unified ideographs extension A, and CJK unified ideographs extensions B. For the mean time, Unicode Consortium is preparing the CJK unified ideographs extension C and CJK unified ideographs extension D. The CJK unified ideographs extension C with 4,251 Han characters will be included into the next version after Unicode 5.1.

For Unicode 4.1, the first block lists the Han characters from [4E00] to [9FBB] in hexadecimal value. The second block lists from [3400] to [4DB5]. The third block lists from [20000] to [2A6D6]. Hence, there are three readily made word lists or character lists for Chinese language. These word lists have 20924, 6582 and 42711 words or characters, respectively. In addition, there are CJK compatibility ideographs having 12 characters. For a combined word list, it is a key space of 70229

characters. After radical exclusion, the key space has about 70000 characters. This forms a Chinese language word list with high entropy of 16.10 bits per Han character.

To start coinware, first flip or toss a coin to randomly select a binary bit "0" or "1". If bit "0", the first and second blocks of CJK unified ideographs and CJK unified ideographs extension A are chosen. If bit "1", the third CJK block of CJK unified ideographs extension B is chosen. Then continue with coin tossing to obtain four coin values representing four binary bits. These four binary bits are converted into one hexadecimal digit. Repeat coin tossing to get four coin values for another three rounds. Four randomly obtained hexadecimal digits will locate the unique Han characters in the previously selected CJK block(s). These three blocks are available at [URL: http://www.unicode.org/charts/]. If the hexadecimal digits do not hit any Han character, get another set of hexadecimal digits.

Coming to here, the selected Han character will need operating system with Chinese language environment to enable computer input. For other languages in Unicode encoding, to create password in those languages needs computing support. The entropy per key in a particular language depends on its character set in Unicode. Nevertheless, for bilingual or multilingual users, larger entropy per key can be obtained, especially when one of the languages is Chinese language.

3.3 Related Work of 2D Key: Single-Line Key/Password Field

Conventionally, whenever secret is used as the authentication method, single-line key field will be the area for a user to enter a key. For the current longest possible key, it is a single-line passphrase. For passphrase, it can be formed from acronym, sentence, diceware, and coinware. Nevertheless, there is a limit due to the problems of memorizability and ASCII character input from keyboard. The first problem is due to the human factor; whereas the second is due to the user interface. These problems prohibit the applications of symmetric key sizes at higher security levels whenever a user cannot remember and/or conveniently enter a long single-line passphrase.

3.4 Key Strengthening

Key strengthening is also called key stretching. It is used to make a weak key stronger. There are two forms of key strengthening. One uses password supplement (Manber 1996; Abadi, Lomas, & Needham, 1997; Abadi, Needham, & Lomas, 2000), and another uses many rounds of hash iterations (Kelsey, Schneier, Hall, & Wagner, 1997). In this thesis, key strengthening is applied to achieve larger protection periods for symmetric and asymmetric cryptosystems like AES and MePKC.

K.-W. Lee (2009b) had a computational analysis on the effect of using key strengthening as presented again as follows.

$$S = n * L * R / P \tag{3.1}$$

S = Key space

n = Number of networked computers

L = Maximum lifetime of a key in years

R = Number of guesses per unit of time per unit of computer

P = Probability that a key can be guessed in its lifetime

Typical values:

$n = 10^9$ units = 29.9 bits

L = 4, 10, 20, 30, 300 years = 2, 28.2, 29.2, 29.8, 33.1 bits

$R = 1.5 \times 10^7\ s^{-1}$ = 23.8 bits (best performance in year 2005)

$R = 1\ s^{-1}$ = 0 bit (using key strengthening)

$P = 10^{-6}$ = -19.9 bits

Equation (3.1) is a password length equation. When key strengthening is used, R becomes 1 guess per second and the variety of computer is a main factor to set the number of hash iterations. The computer performance of a variety of computers

varies from 1 time for the slowest computer to 20 times for the fastest computer. This contributes a factor of $\log_2 20 = 4.3$ bits to Equation (3.1). Moore's Law states that the number of transistors on an integrated circuit for minimum component cost doubles every 24 months.

$$S = (n * L * R / P) * 2^{4.3} * 2^{L/2} \quad (3.2)$$

When the variety of computers and Moore's Law are considered, it becomes Equation (3.2). From Equation (3.2), key strengthening can make a weak key to become 19.5 bits stronger.

3.5 Memorizable Secret as a Master Key

3.5.1 Introduction

For friendly environment, cost effectiveness, and efficiency, human civilizations are heading towards a paperless and electronic society. Every human is getting numerous offline and online accounts. These accounts require authentication to gain system access. There are four types of authentication approaches: Secret, token, biometrics, and introducer.

Secret is about something you know like password or key. Token is about something you have like smart card. Biometrics is about something you are like fingerprint. Introducer is whom you know. For the sake of cost and compatibility, secret in the form of key is the most popular authentication approach.

According to Forrester Research (Kanaley, 2001), an active Internet user manages an average of 15 keys on a daily basis. Most people, who are majority-wise, not using the password management tools, either maintain the same key for all the accounts, write down different keys for different accounts, or keep closely related keys for various accounts. These are all poor password management practices.

The HTTP basic authentication protocol (even over SSL) (Franks, Hallam-Baker, Hostetler, Lawrence, Leach, Luotonen, & Stewart, 1999) allows a server to

know the key of each account. This causes possible malicious server attacks from the administrators and crackers. The server may be untrustworthy or compromised.

For another HTTP specification, i.e. HTTP digest authentication protocol, challenge-response protocol is used (Franks, Hallam-Baker, Hostetler, Lawrence, Leach, Luotonen, & Stewart, 1999). The server can still see the clients' keys. Since the response from a client to a server is not specific to the server, HTTP digest authentication protocol is vulnerable not only to malicious server attacks, but password file compromise attacks, spoofing attacks, and phishing attacks.

If a key is reused, the success of an attack on an account in a weak system may cause a strong system to be compromised. This password reuse can trigger a domino effect from the weakest system to the strongest system (Ives, Walsh, & Schneider, 2004).

Therefore, every key has to be uniquely set for each account, regardless of weak or strong system, to get rid of the risk when one system is compromised. However, according to (Adams & Sasse, 1999), normal users can only be expected to cope with a maximum of four or five keys that are unrelated and regularly used. When key relevancy is allowed, a user can cope with average 6.5 unique keys (Florencio & Herley, 2007). This reflects the need to balance the usability and security.

To address this problem, some key management tools are invented. These tools allow users to remember only one master secret as master key and assign unique slave keys (aka site keys) to multiple accounts. They allow users either to choose their own master key and then store the slave keys somewhere safe, or to assign fixed keys to each website that can be computed whenever they are needed.

The examples of the first approach are Password Safe and Windows Live ID. The examples of the second approach are LPWA (Lucent Personal Web Assistant), HP Site Password, Password Multiplier, SPP (Single Password Protocol), PwdHash, and Passpet. A special example using the hybrid approach is CPG (Compass Password Generator).

Password Safe is a password vault that can be used for offline and online accounts. However, its mobility is low due to the requirement to have a safe storage

for multiple keys encrypted by a common master key. Another form of solution for online accounts only is to use a single sign-on server and its proxy servers. Microsoft Windows Live ID (aka Microsoft Passport Network) is one of these examples. Its weaknesses are single point of failure and high cost of integration.

Another method to reduce the memory burden of online account passwords uses key hashing and key strengthening (aka key stretching) of a master key concatenated with a domain name and optional username. Exemplary applications of this method are (i) LPWA (Lucent Personal Web Assistant) (Gabber, Gibbons, Matias, & Mayer, 1997); (ii) HP Site Password (aka System-Specific Passwords or Site-Specific Passwords) (Karp & Poe, 2002; Karp, 2003); (iii) Password Multiplier (Halderman, Waters, & Felten, 2005); (iv) PwdHash (Ross, Jackson, Miyake, Boneh, & Mitchell, 2005); and (v) Passpet (Yee & Sitaker, 2006).

There is also a method using unique random number assignment to different online accounts called CPG (Compass Password Generator) (aka Common Password Method) (Luo & Henry, 2003). Yet there is another method using the key hashing of one-time ticket, server name, and master password to generate different site keys (aka slave keys) called SPP (Single Password Protocol) (Gouda, Liu, Leung, & Alam, 2005).

All these methods of single master key generating multiple site keys or slave keys apply only to online accounts having a domain name. Its weakness is a change of master key requires all the accounts to be updated one by one, which is required by some key management strategies.

For offline account, the current prior art uses a password vault to store all the unique passwords the secret. These password vaults can be simply an encrypted spreadsheet or document file, or application software like Password Safe by Bruce Schneier [URL: http://www.schneier.com/passsafe.html]. The disadvantage of password vault is its low mobility and danger of disclosing the ciphertext of password vault to the public domain. Hence, there exists a need to have a method to generate multiple slave keys of online and offline accounts from a master key, and yet an individual slave key can be changed without changing the master key and other slave keys.

With the realization of big memorizable secret for cryptographic, information-hiding, and non-cryptographic applications, especially MePKC, there are even more types of offline accounts like symmetric key, asymmetric private key, stego-key, symmetric watermarking key, asymmetric watermarking private key, and PRNG seed. Among them, for MePKC cryptographic applications like encryption, signature, authentication, key exchange, and other schemes, different schemes require a different pair of asymmetric key pair, by the technical and law requirements to have a safer electronic information society. Hence, there exists a need to generate multiple private keys as slave keys from a common memorizable master key.

The present invention called multihash key (Lee & Ewe, 2007) can be applied to offline and online accounts with good mobility. Domain name is not necessary but optionally needed to resist phishing attacks and spoofing attacks. A single sign-on server is also not needed. The required components are numeric 4-digit passcode, key hashing, key strengthening, and hash truncation.

To allow diversity of site keys from a single master key, there are two optional entries: Username ID and domain name (or website) URL. Domain name that is also used to resist phishing attacks can be replaced by adopting an anti-phishing tool. In other words, the proposed new method and system can be used together with an anti-phishing tool.

These anti-phishing tools are SpoofStick, Netcraft Toolbar, Earthlink Toolbar, SiteKey, DSS with SRP (Dynamic Security Skins with Secure Remote Password Protocol), Petname Tool, TrustBar, and Passpet (Yee & Sitaker, 2006).

3.5.2 Related Works

Here, the prior arts of key management tools are discussed, where a single key can be used for multiple accounts, in a deeper context. Anti-phishing tools will not be discussed. Accounts are divided into two types: Offline and online. Offline accounts have no domain name while online accounts have domain name. Example of offline accounts is file encryption; whereas example of online accounts is email.

Password Safe is an application software originally developed by Bruce Schneier [URL: http://www.schneier.com/passsafe.html]. It uses the Twofish encryption algorithm to protect the stored passwords by a master password. Users need only to remember one master password to access multiple passwords. Its mobility depends on the available password database. It can be used for both offline and online accounts, but cannot resist spoofing attacks and phishing attacks.

Windows Live ID (No date) is also known as "Microsoft Passport Network" [URL: http://www.passport.net]. Users need a master password to sign on a central server. This central server will authenticate users for multiple servers which have joint network. Besides single point of failure, it has high cost of integration. Some security loopholes are reported (Kormann & Rubin, 2000). It can be used for online accounts only, but can resist phishing and spoofing attacks.

LPWA (Gabber, Gibbons, Matias, & Mayer, 1997; Matias, Mayer & Silberschatz, 1997) uses key hashing of master password and domain name to generate a specific site password via a server. It has single point of failure but not the high cost of integration. However, the malfunction of central authority will mean the breakdown of all services. It can be used for online accounts only and can resist phishing and spoofing attacks. Nowadays, it has stopped providing the services.

HP Site Password (Karp, 2003; Karp & Poe, 2004) is also called "System-Specific Passwords" or "Site-Specific Passwords". A master password and a system name are concatenated, hashed using MD5 (Rivest, 1992) and converted into Base64 encoding (Borenstein & Freed, 1992) to get a site password. It is not centralized using a server but operates as stand-alone application in the terminal computers. It can be used for online accounts only and cannot resist phishing and spoofing attacks.

It is important to note here there were few successful collision attacks over the MD5 in the years 2004-2006. The successor of MD5, which is SHA-1, is also discovered to be subject to collision attacks on its reduced version in the years 2004-2006. Consequently, NIST announced that SHA-1 would be phased out by the year 2010 in favour of SHA-2 variants: SHA-224, SHA-256, SHA-384, and SHA-512 (NIST, 1995a, 2002b, 2007b; Lilly, 2004).

CPG (Luo & Henry, 2003) is also called "Common Password Method". It assigns unique random numbers to different website accounts. The random number is hashed using MD5 and converted using a binary-to-text transform to generate a specific password for multiple accounts. The random number is encrypted and stored in an account server or proxy server. When a user needs to access a specific account, the encrypted random number is retrieved from the server, decrypted, hashed, and converted into a specific password to authenticate the access. Therefore, it has the weakness of single point of failure, but does not involve the high integration cost like LWPA. It is for online accounts only and can resist phishing and spoofing attacks.

Password Multiplier (Halderman, Waters, & Felten, 2005) uses key hashing and key strengthening. There are two levels of hash iterations using the inputs of username, master password and site name. Both the numbers of hash iterations are fixed for 100 seconds and 1/10 second, respectively. It is a stand-alone application without using a server and implemented using browser extension to Mozilla Firefox. It can be used for online accounts only and can resist phishing and spoofing attacks.

SPP (Gouda, Liu, Leung, & Alam, 2005) is also a stand-alone application. It applies the techniques of challenge-response protocol, one-time server-specific ticket and key hashing using MD5 or SHA-1. The site password is hashed from the one-time ticket, server name, and master password. The one-time ticket and site password will be updated after every login access. It can be used for online accounts only and can resist phishing and spoofing attacks.

PwdHash (Ross, Jackson, Miyake, Boneh, & Mitchell, 2005) is implemented using browser extensions to Mozilla Firefox, Internet Explorer, and Opera. Its key hashing inputs the domain name of remote site into a pseudo-random function controlled by user's master password. The domain name acts as a hash salt. It can be used for online accounts only and resist phishing and spoofing attacks.

Passpet (Yee & Sitaker, 2006) is also implemented using browser extension to Mozilla Firefox. It applies the techniques of petname system, key hashing, key strengthening, and UI customization. Petname system is a naming system possessing the properties of globality, security and memorizability. It is used for anti-phishing attacks. Key hashing and key strengthening in Passpet are alike the Password

Multiplier using the SHA-256, except that its first level of hash iterations is flexible in amount allowing updates according to the computer technology advancement without changes of software. It uses local storage for login access via a fixed machine, and remote storage in a server for login access with mobility feature. The remote server stores the first level of hash iterations and site label file that is encrypted from the site label list. Due to the dependency of server for newly used machines, Passpet has some risks of single point of failure. However, there is no high cost of integration. It can be used for online accounts only and can resist phishing and spoofing attacks.

3.6 Related Works of MePKC: Storages of Private Key

For the current asymmetric key cryptosystem, a private key is normally encrypted using another symmetric key. The encrypted private key is stored in a local computing system or token; whereas the symmetric key is stored in the human brain. The present possible attacks for this method are guessing attack, dictionary attack, and pre-computation attack.

Another method is to split the private key into two or more portions (Ganesan, 1996b; Bishop, 2003, pp. 264-265). There are other literary works about split private key cryptography over here (Ganesan, 1996a, 1998a, 1998b, 1998c, 1999; Ganesan, Sandhu, Cottrell, & Austin, 2006a, 2006b, 2006c; Ganesan, Sandhu, Cottrell, Schoppert, & Bellare, 2006; Ganesan & Yacobi, 1996; Sandhu, deSa, & Ganesan, 2003, 2005a, 2005b, 2005c, 2006a, 2006b, 2006c, 2006d, 2006e, 2006f; Sandhu, Schoppert, Ganesan, Bellare, & deSa, 2006a, 2006b, 2006c, 2006d, 2006e, 2006f, 2007a, 2007b, 2007c, 2007d; Sandhu, Ganesan, Cottrell, Renshaw, Schoppert, & Austin, 2007). The first portion of the private key can be derived from a normal human-memorizable symmetric key. The other portions of the private key are stored as encrypted partial private key alike the normal encrypted private key. This method resists the pre-computation attack.

A third method is to store the encrypted private key in a server connected to a computer communication network, called roaming private key (Baltzley, 2000, 2001a, 2001b). A user has the roaming capability where the encrypted private key

can be downloaded from the server for decryption at anywhere. Proxy servers are needed for this method to avoid single point of failure. Its possible attacks are the same as encrypted private key stored in the local computing system.

3.7 Related Prior Arts of Tools to Resist Hacking

Besides complicated networking settings and firewall software, a simple hardware device was proposed by Fonseca (2003) by using a simple push/pull level of a switch box to connect or disconnect the networking connection for the hacking elimination. Fonseca called it as data line switch and filed for patent in the US on 24 July 2001. Later, Macuch (2005) designed the data line switch for the applications of coaxial and DSL cables to control the computer connection to the Internet. Macuch filed for a design patent in the USA on 17 November 2003. Of course, there is yet another current practice by some end users to plug and unplug the networking cable. Nevertheless, this method suffers from the hook damage of RJ45/RJ11 and inconvenience access of networking port.

Here later, a proposed component with similar function to data line switch is also applicable to modular jack (aka modular connector) like RJ45 and RJ11. Modular connector was firstly invented by Hardesty (1975), who filed it for patent in the US on 6 July 1973. RJ stands for registered jack. RJ45 and RJ11 are used as Ethernet jack and telephone jack, respectively. Our new component is innovated from the dual in-line package (DIL/DIP) switch by adding a collective actuator, which can be slide-type, rocker-type, or piano-type (aka side/level).

The miniature DIP switch was found in the US patent database to be firstly invented by Lockard (1977, 1979), who filed for patent in the US on 25 March 1975 for the first time. Since then, there are various innovations on the DIP switch. Hoffman (1982) had improved the manufacturing of DIP switch. Liataud and Maloney (1983) had reduced the size, decreased the cost, and increased the reliability of DIP switch. Brown (1983) had created the piano-type DIP switch. In the late decade, Lin (1999) and Tai (2001) from Taiwan, R.O.C., had concomitantly decreased the size, improved the manufacturing process, and increased the reliability of DIP switch.

Normal slide switch wipes in parallel with the pin pairs. The slide actuator of my proposed component wipes transversely to the pin pairs. The first slide switch that can be found in the US patent database was invented by Bailey (1969). Even though the wiping directions of normal slide switch and our switch are different by 90^0 degrees, their function is the same, i.e. to connect and disconnect the poles, except the 10-way secure DIP switch oppositely switches two groups of poles.

3.8 Conclusion

Till here, we have discussed the prior arts and related works to all the four main novel works proposed by me, in which they are (i) *2D key* for big and yet memorizable secret; (ii) *multihash key* for multiple offline/online slave keys from one master key the big memorizable secret; (iii) *MePKC* for various public key cryptographic schemes using fully memorizable private key; and (iv) *anti-hacking data storage using improved DIP switch* for secure storage of original plaintext and decrypted ciphertext from virtual hacking over the computer communication networks. All those four major novel knowledge contributions here can act as a whole for safer and more convenient electronic computer communications.

CHAPTER 4 RESEARCH METHODOLOGY (PART 1): CREATING BIG MEMORIZABLE SECRET USING TWO-DIMENSIONAL (2D) KEY

4.1 Introduction

Conventionally, single-line key field is used to input a key. The selection of a key depends on the factors of memorizability and security. The minimum key sizes for symmetric and asymmetric key cryptosystems are 80 and 160 bits, respectively.

For symmetric key cryptosystem, National Institute of Standards and Technology (NIST) of USA proposed security level of 80-bit key to be phased out by year 2015 and used until year 2010 (E. Barker, W. Barker, Burr, Polk, & Smid, 2007a, 2007b). US government has an export policy to control the power of cryptographic algorithm by setting the maximum key size. The current export limit of symmetric key size has been raised from 40 bits to 128 bits.

For the symmetric key cryptosystem of Advanced Encryption Standard (AES), there are three key sizes: 128, 192, and 256 bits. The asymmetric key cryptosystems, which demand for the minimum private key size at 160 bits by year 2010, are finite field cryptography (FFC) and elliptic curve cryptography (ECC). FFC and ECC are based on the mathematical hard problems of discrete logarithm problem and elliptic curve discrete logarithm problem, respectively. The corresponding sizes of private keys to the AES are 256, 384, and 512 bits, respectively (E. Barker, W. Barker, Burr, Polk, & Smid, 2007a, 2007b; Gehrmann & Näslund, 2005, 2006, 2007). The symmetric key is normally remembered by brain; whereas the asymmetric private key is encrypted using another symmetric key.

ASCII characters have absolute entropy of 6.57 bits per character. Therefore, the nominal bit of an ASCII character is 8 bits, but its effective bit is 6.57 bits. To cater for the different symmetric key sizes at 80, 96, 112, 128, 192, and 256 bits as in Table 2.3, 13, 15, 18, 20, 30, and 39 ASCII characters are needed, respectively. An amount of 15 ASCII characters is perhaps still affordable and convenient for the human users. However, higher amounts may introduce two problems.

Memorizability is the main problem. The difficulty to type a long passphrase into a computer will be another open problem (Schneier, 1996).

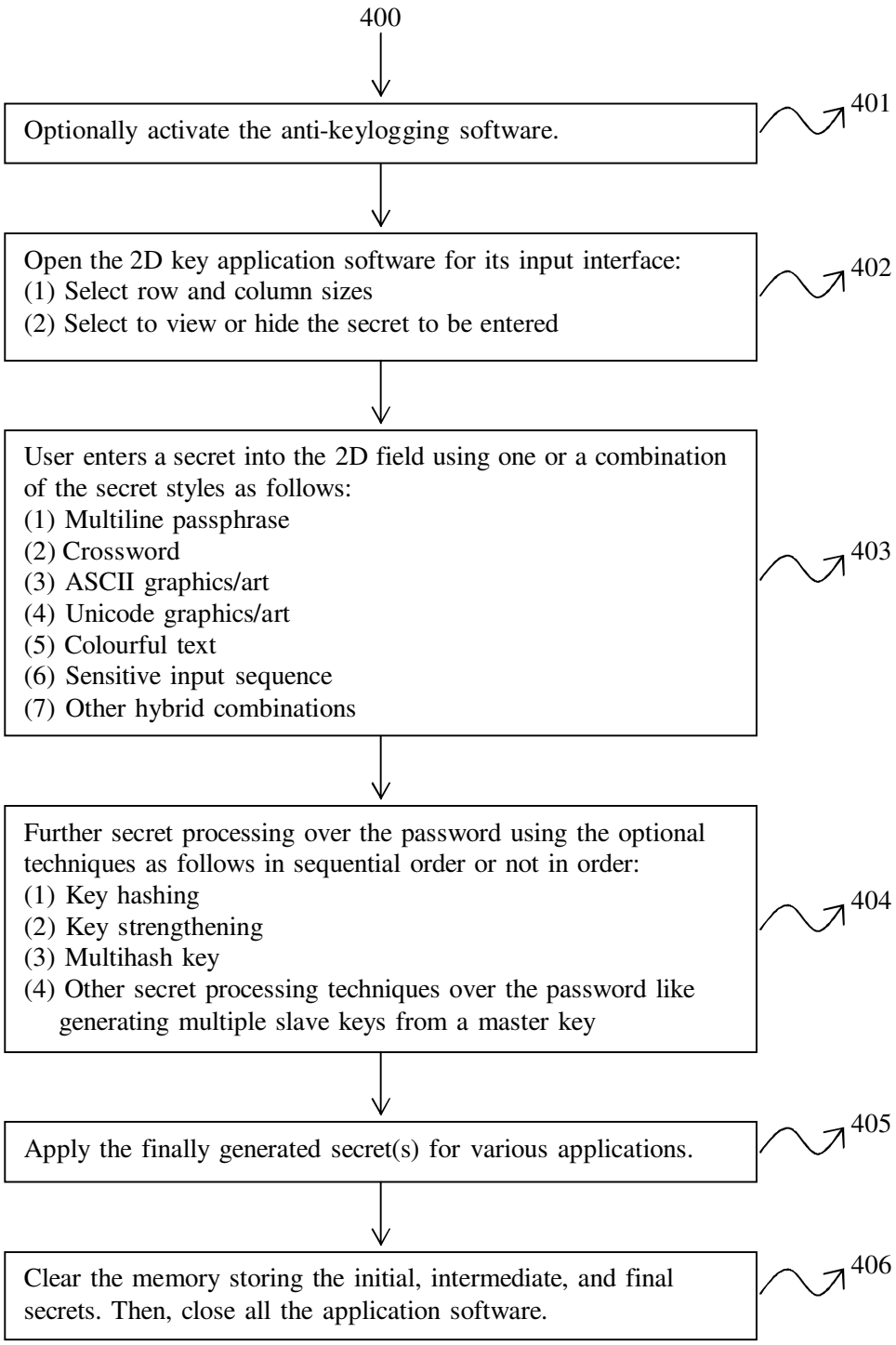


Figure 4.1 Operation of 2D key input method and system

Here, a high-entropy key input method called 2-dimensional (2D) key as in Figure 4.1 is proposed to solve these problems. 2D key facilitates particularly the recognition of reference points of each sub-unit of a passphrase, and generally the creation of various secret styles of 2D key like multiline passphrase, crossword, ASCII graphics/art, Unicode graphics/art, colourful text, sensitive input sequence, and two or more of their hybrid combinations as partially illustrated in Figures 4.3-4.6, for Latin language users.

It uses a 2D display as user interface to improve the human factors of memorizability and input of ASCII characters from keyboard. The 2D key has the styles of multiline passphrase, crossword, ASCII art, colourful text, or sensitive input sequence. It can resist dictionary attack and fulfil the demands of human-memorizable key sizes even until 256 bits, which is impossible by using the single-line passphrase.

In addition to fulfilling the various key sizes of symmetric key cryptosystem, 2D key has novel revolution to the private key storage of asymmetric key cryptosystem. For the prior arts, we have encrypted private key, split private key, and roaming private key. With the introduction of 2D key, there shall be no more need to store the private key in a computing system, but inside the brain as like the symmetric key. This allows the creation of memorizable public-key cryptosystem (MePKC) as discussed in Chapter 6. MePKC has the special features of mobility, lower cost, and higher efficiency.

4.2 2D Key Input Method

For single-line passphrase, the numbers of ASCII characters for different symmetric key sizes are shown in Table 2.3. An amount of 15 ASCII characters or 96 bits is a maximum memorizability limit for many human users. This fact is statistically proven by Florencio and Herley (2007) in their large-scale study of web password habits for half a million users over a 3-month period, where the average key size is 40.54 bits ranging from exclusive 0 to inclusive 100 bits or]0, 100]. The

difficulty of user interface to enter a key using keyboard into the single-line key field is another big problem.

The problems of human factor and user interface limit the practical application of symmetric key cryptosystem to be at the key size of 96 bits with 10 years of protection. Using key strengthening, the 96-bit key can be made 19.5 bits stronger, and 20-year protection is the maximum theoretical limit.

The 2-dimensional (2D) key input method is created to allow high-entropy keys. Figure 4.2 displays the pseudocode of 2D key input method. It tries to solve the human factor of memorizability and user interface of key input. 2D key has a 2-dimensional display alike a 2D matrix, where each character of a key is an element of the matrix. The key styles drawn in the space of 2D matrix are a mixture of 2D text in pictorial form. Thus, 2D key can create big and yet memorizable secret.

```
1.0 User selects row size.
2.0 User selects column size.
3.0 User enters ASCII characters or Unicode symbols one by one.
4.0 User ends the key input by pressing the “Enter” key.
5.0 Computer hashes the input key.
6.0 Computer compares the hashed key with the stored hash.
        6.1 If the hashes match, authentication is verified.
        6.2 If the hashes mismatch, authentication is rejected.
```

Figure 4.2 Pseudocode of 2D key input method and system

The font used for 2D key has to be fixed-width font. Fixed-width font is also called non-proportional font and monospaced font. It is a typeface using fixed width for every glyph. Examples of fixed-width fonts are *Courier* for ASCII and *MS Mincho* for Unicode. When ASCII encoding is used, the 2D key has 6.57 bits per character. Meanwhile, when Unicode is used, it has 16 bits per character. Even though Unicode-based 2D key has higher entropy, it is inconvenient to enter a Unicode symbol for the mean time, and the fixed-width font for all the Unicode symbols has not yet been created. Hence, ASCII-based fixed-width font is used currently for the discussions as well as prototype demonstration.

To use 2D key input method and system, firstly a user needs to select the row size and column size of the 2D matrix for 2D key. The currently built prototype has a maximum row size or height of 10 characters, and a maximum column size or width of 13 characters. The column size is set at 13 due to the Chinese-character-encoded passphrase (Lee, 2009a) has a maximum size of 13 per Chinese character. Alternatively, it can be a word in English language or other languages that has a size of 13 characters per word with character stuffing.

The input styles of 2D key are multiline passphrase, crossword, ASCII art, Unicode art, colourful text, and sensitive input sequence. Multiline passphrase, crossword, and ASCII art are currently implemented in the prototype; whereas Unicode art, colourful text, and sensitive input sequence require additional supports.

After selecting the row size and column size, the user can input ASCII characters using keyboard as the elements of the 2D matrix. The input characters can have any style or a mixed style of 2D key. These styles have good memorizability, and the 2D nature of 2D key generates more references at the user interface for key input. Single-line key field has only one reference at the first location of the only line. 2D key has a number of horizontal lines and each first location of the horizontal lines acts as references for key input. In addition, the first locations of the vertical lines can be secondary set of references for key input. This solves the location recognition problem of user interface in facilitating a user to enter a high-entropy key by having more indexed references.

Good memorizability allows a user to repeat a high-entropy key. The elements of 2D matrix can be either partially, fully, or extraordinary filled. To fill extraordinarily means adding some extra trailing characters as noise (Lee, 2009a) after the last element of the 2D matrix. The characters entered into the 2D key field are read by a computer line by line horizontally from top to bottom, hashed, and processed as usual alike the single-line key field. The hashing process is one round if key strengthening is not used. If key strengthening is used, the hashing iteration is set according to the computer response time per access ranging from 0.05 to 1 second, or any other tolerable ranges.

4.3 Styles of 2D Key: Multiline Passphrase

For single-line key field, it is hard to input a high-entropy single-line passphrase due to the problem of user interface. A user may lose the reference of starting character of a word in a passphrase. Using 2D key, multiline passphrase can be input, where each line consists of one word of a passphrase. Each word is padded to the longest word in the passphrase. The padding character can be any ASCII character and acts as a text-based semantic noise (Lee, 2009a). Figure 4.3 shows a 2D key example using multiline passphrase. Its dimensions are 4 x 5, and uses character '*' as the padding character. This 2D key has absolute entropy of 131 bits.

```
Have*
a****
happy
day!*
```

Figure 4.3 Styles of 2D key: Multiline passphrase

```
HAPPY*
O*R*K*
M*INCH
E*D*U*
SPELLS
```

```
WELCOME
:TO::::
::USE::
::::2D:
::::KEY
```

Figure 4.4 Styles of 2D key: Crossword

4.4 Styles of 2D Key: Crossword

The second style of 2D key is crossword. Instead of horizontal and vertical multiline passphrase, a user can enter a mixture of horizontal, vertical, and slanted passphrases. Figure 4.4 shows two 2D key examples using crossword. Their dimensions are 5 x 6 (left) and 5 x 7 (right), and use characters '*' and ':', respectively, as the background character. These 2D key have absolute entropy or key size of 197 and 229 bits, respectively.

4.5 Styles of 2D Key: ASCII Art / Unicode Art

The third style of 2D key is ASCII art or Unicode art. ASCII art is a graphical presentation of computer using the 95 printable ASCII characters. Unicode is a variant of ASCII art, where instead of using ASCII characters, Unicode symbols are used to create artistic graphics.

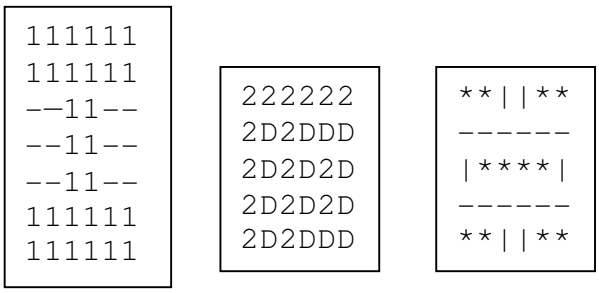


Figure 4.5 Styles of 2D key: ASCII art

Figure 4.5 displays three 2D key examples using ASCII art. For the left example, ASCII characters '1' and '-' are used to display a Chinese character meaning "engineering". Its dimensions are 7 x 6 with key size of 275 bits. For the middle example, ASCII characters '2' and 'D' are used to display a digit '10' with background character '2'. Its dimensions are 5 x 6 with key size of 197 bits. For the right example, ASCII characters 'I' and '-' are used to display a Chinese character meaning "centre" with background character '*'. Its dimensions are 5 x 6 with key size of 197 bits.

Figure 4.6 shows a 2D key example using Unicode art. Unicode symbols '¥' and '©' are used to display a Chinese character meaning "engineering" again. Unicode '¥' is entered using the keyboard by pressing the keys "0165" while holding the key of 'Alt'. Unicode '©' is entered using the keyboard by pressing the keys "0169" while holding the key of 'Alt'. Once the 'Alt' key is released, the Unicode symbol is entered. Its dimensions are 4 x 5. This 2D key has key size of 320 bits.

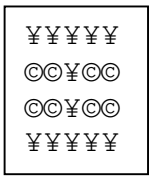


Figure 4.6 Styles of 2D key: Unicode art

4.6 Styles of 2D Key: Colourful Text

The style of this 2D key needs some additional supports. Colour encoding, special graphical user interface, and special computer processing are required. Although these supports make the user interface complicated for the computer, they can be implemented and have better memorizability for the human users. Colour is definitely a main element of good memorizability. For example, by having 16 types of colours, every character in the 2D key will have an additional 4 bits. ASCII-based 2D key will become 10.57 bits per character; whereas Unicode-based 2D key is 20.59 bits per character. The entropies per character of ASCII-based and Unicode-based 2D keys will be increased by 60.9% and 24.1%, respectively. The additional colour secret also carries more randomness to resist dictionary attack.

4.7 Styles of 2D Key: Sensitive Input Sequence

For the secret style of sensitive input sequence, it is an additional feature over the current 2D secret style where there is added entropy from the input sequence of a character to a specific element location of the 2D matrix. If a 2D key has the dimensions of m x n, the key space is increased by [$(m * n)!$]. If a 2D key of 4 x 5 as in Figure 4.3 is used, the key space is increased by [20!] or 61.1 bits from 131.40 bits to 192.47 bits, which is close to the left example in Figure 4.4 for the 2D key of dimensions 5 x 6 with 197.10 bits.

This key style requires the space encoding for the element location of 2D matrix, table-like graphical user interface of m x n matrix, and human memory for the sequence of characters. In term of memorizability, there is not much improvement. However, the time to enter a 2D key of similar size is greatly reduced for the same amount of key size.

4.8 Requirement of Key Size for 2D Key

Table 4.1 shows the setting sufficiency of various dimensions of 2D key as compared with ASCII-based and Unicode-based passwords for various key sizes.

Based on enough key size by using 2D key, different levels of security strength for symmetric key cryptosystem like AES-128, AES-192, and AES-256 can be practically realized. For fully mnemonic private key, maximally easily achievable MePKC is FFC-256 and ECC-256. For 512-bit MePKC, more conditions for 2D key are needed, in which it may restrain to a specially trained human group.

Table 4.1 Various key sizes corresponding to the numbers of ASCII characters, Unicode (version 5.0) characters, and settings sufficiency of 2D key input method

Key size (bit)	80	96	112	128	160	192	256	384	512
Number of ASCII character (6.57 bits)	13	15	18	20	25	30	39	59	78
Number of Unicode character (16.59 bits)	5	6	7	8	10	12	16	24	31
ASCII-based (4 * 5) 2D key (131.4 bits)	Yes	Yes	Yes	Yes	No	No	No	No	No
ASCII-based (5 * 6) 2D key (197.1 bits)	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
ASCII-based (7 * 6) 2D key (275.9 bits)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	No
Unicode-based (5 * 5) 2D key (414.8 bits)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No

CHAPTER 5 RESEARCH METHODOLOGY (PART 2): MULTIHASH KEY

5.1 Overview

A human's e-life needs multiple offline and online accounts. It is a balance between usability and security to set keys or passwords for these multiple accounts. Password reuse has to be avoided due to the domino effect of malicious administrators and crackers. However, human memorizability constrains the number of keys. Single sign-on server, key hashing, key strengthening, and petname system are used in the prior arts to use only one key for multiple online accounts. The unique slave keys (aka site keys) are derived from the common master secret and specific domain name. These methods cannot be applied to offline accounts such as file encryption. New method and system are invented to be applicable to offline and online accounts. It does not depend on http server and domain name, but numeric 4-digit passcode, key hashing, key strengthening, and hash truncation. Domain name is only needed to resist spoofing and phishing attacks of online accounts.

5.2 Introduction

There are lots of situations that require a user to have many online and offline accounts. Examples of online and offline accounts are login access and file encryption, respectively. For safer security, a secret cannot be re-used to avoid password domino cracking effect (Ives, Walsh, & Schneider, 2004), where an attacker starts the password cracking process from the weakest link. However, according to R. Kanaley (2001), an Internet user manages an average 15 keys on a daily basis. Yet in another survey by Adams and Sasse (1999), a user can only be expected to handle 4 to 5 unrelated and regularly used keys. For user's unique keys without the constraint of relevancy, Florencio and Herley's survey (2007) reported an average 6.5 keys, repeated 3.9 times each for 25 accounts and typing 8 keys daily. Hence, there is a memory burden to the user unless these secrets are written down

somewhere. However, important password the secret is discouraged to be jotted down somewhere.

5.3 Basic Model of Multihash Key

The proposal here requires users to remember an at least 128-bit master key and a numeric 4-digit passcode. The master key can be derived from creation methods of big memorizable secret (Lee, 2008h, 2008k, 2008l, 2009a, 2010b, 2010c), like 2D key. This method and system is named "multihash key".

The passcode is used together with key hashing, key strengthening (Manber, 1996; Abadi, Lomas, & Needham, 1997; Abadi, Needham, & Lomas, 2000; Kelsey, Schneier, Hall, & Wagner, 1997) and hash truncation to generate exemplary 20 unique hashes at 20 security levels for 20 accounts. Each security level has 1 account. These hashes are site keys. All the security levels are ranked from the highest security (#1) to the lowest security (#20). This is because knowing the multihash key at the higher level can reveal the multihash key at the lower level, but not the reverse, through partial brute-force attack via guessing.

From Kanaley's survey (2001), 20 accounts are set since an active Internet user manages an average of 15 keys daily. Five accounts are added by assuming that there are five offline accounts. The number of accounts can be increased by changing the settings or remembering another pair of (master key, passcode).

There are three pseudo-codes for multihash key to show how the method and system work: Determination of hash iterations of multiple security levels, generation of multihashes as site keys, and changes of key pair (master key, passcode).

As an example, Figure 5.1 shows the determination of 20 security levels via the experiments to locate the lower bound b_L and upper bound b_H for 1-second hash iterations for an old computer that is slow but still popular in early years of 2000 AD. Each security level is partitioned by 2^8.

Figure 5.2 presents the basic model of multihash key to generate multihashes as site keys. A user needs to remember the selected security level for a specific account. In case of forgetfulness, all the 20 security levels shall be tried one by one.

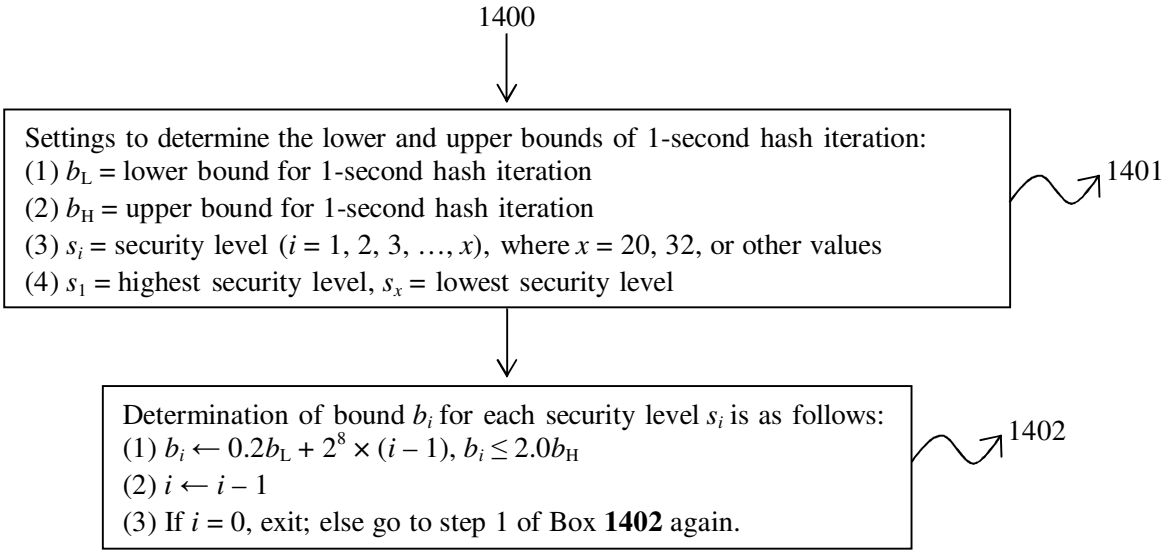


Figure 5.1 Pseudo-code to determine the numbers of hash iteration for multiple security levels of multihash key methods and systems

Necessary entries are master key d and numeric 4-digit passcode d_N. Optional entries are username ID and website (or domain name) URL. The username and website are used to create diversity of multihash key from a key pair (master key, passcode). Domain name can also help to resist phishing and spoofing attacks.

The 512-bit hash of the concatenated master key and passcode is truncated into 20 partitions with 8-bit each from the MSB bit. This increases the randomness of specific keys for different accounts. If an attacker does not know the exact security level, then 5120 (= 2^8 * 20) hashes have to be checked for any key pair (master key, passcode). If the attacker knows about the security level, then 2^8 hashes have to be validated for any key pair (master key, passcode).

For the settings of bound b_i, it can be either fixed or random. If the fixed option is chosen, the number of hash iterations will use the standard settings. A user is mobile and can use this method without remembering the number of hash iterations while accessing offline and online login account from different computing systems.

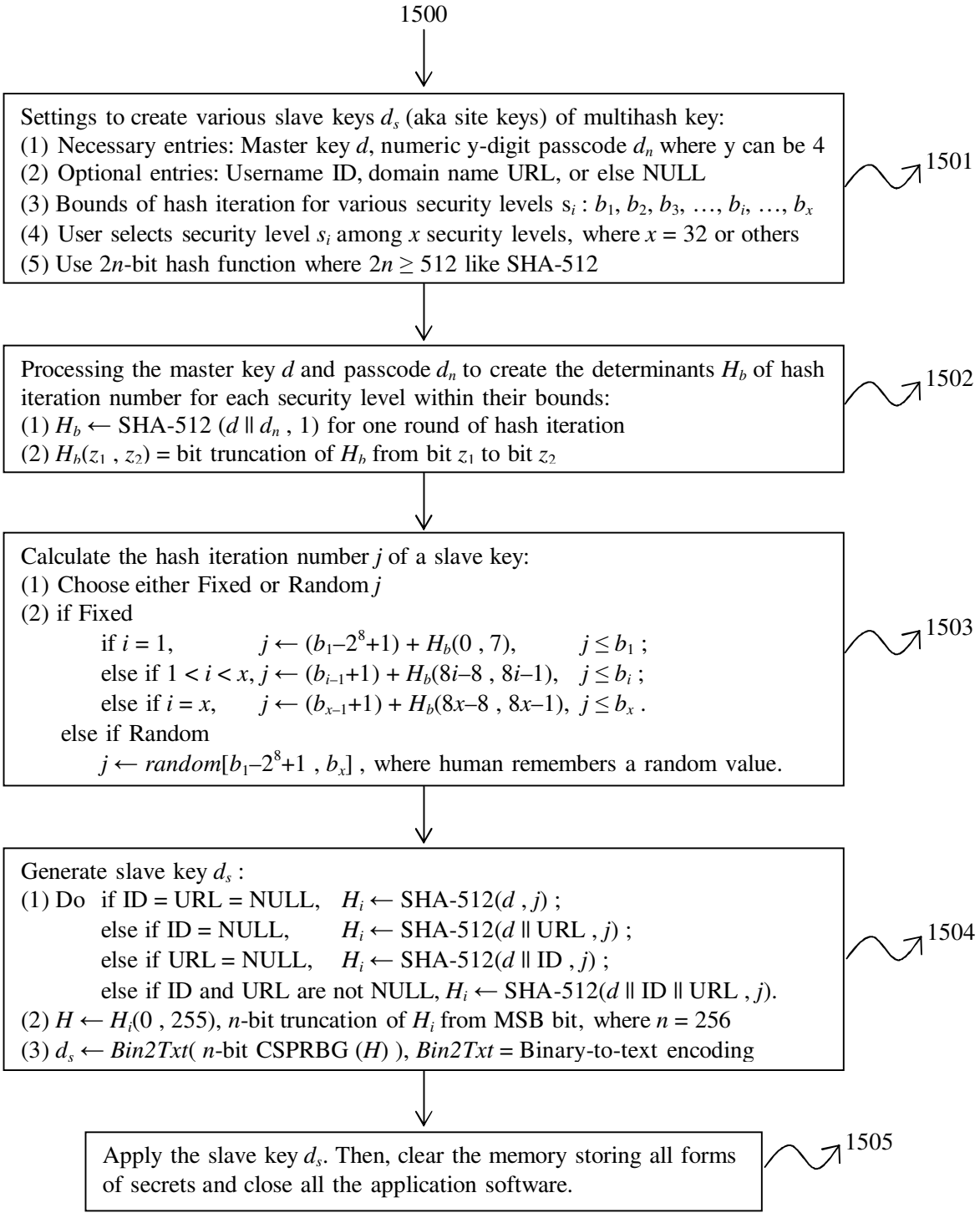


Figure 5.2 Operation of the basic model of multihash key method and system

If the random option is chosen, the number of hash iterations will be randomly selected by a user within a given range. User's mobility is weakened unless one can remember the random values of hash iterations while accessing offline and online logins. However, if a user can remember the hash iterations, this option offers stronger resistance to dictionary attack. The best option is a hybrid scheme. Choose fixed option for lower security levels and random option for higher security levels.

Depending on the value existence of username ID and domain URL, the master key undergoes different key hashing and key strengthening using SHA-512 to generate hash H_i. H_i is then encoded from binary to text to fulfil the demands of password requirements such as alphanumeric, mixed lowercase and uppercase, and with punctuation marks.

Table 5.1 Binary-to-text encoding Bin2Txt(H) of multihash key

Bin	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
Txt	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
Bin	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Txt	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Bin	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47
Txt	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
Bin	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
Txt	!	“	#	$	%	&	‘	(	)	*	+	,	-	.	/	@
Bin	Padding															
Txt	~															

N.B.: Bin: For easy understanding, decimal value is shown to represent binary values

Here, a binary-to-text encoding of *Bin2Txt*(*H*) is proposed as in Table 5.1. Base64 encoding is not used as there are only two punctuation marks included (Borenstein & Freed, 1992). *Bin2Txt*(*H*) converts 6 binary bits into one 8-bit ASCII

character. It has a bit expansion of 33%. All types of ASCII characters are included: lowercase, uppercase, digit, and punctuation marks. The last group of 4 binary bits of *H* from 253rd to 256th is padded with 2 binary bits of 0 at the right or LSB side. The output of *Bin2Txt*(*H*) is a string of 43 ASCII characters and is used as key hash.

Lastly, copy the hash as site key into the clipboard and paste it on the prompt key field for authentication access. **Remember to clear the clipboard before leaving the computer.**

On how to change from an old key into a new one, a user can change either the master key, passcode, security level, username, or the domain name. There are also proposed usages of 20 security levels as shown in Figure 5.3.

Security levels: usages
1 Password file and key management tool like password vault.
2 Finance => Very important Internet banking.
3 Finance => Important Internet banking.
4 Finance => Stock trading.
5 Finance => Insurance, income tax, ...
6 Very important personal encrypted files, email accounts, instant messengers, …
7 Important personal encrypted files, email accounts, instant messengers, …
8 Very important accounts in working/studying place like email.
9 Important accounts in working/studying place like database.
10 Other accounts in working/studying place like library.
11~20 Other not frequently used offline and online accounts.

Figure 5.3 Proposed usages of 20 security levels

New methods and systems called multihash key and its variants are presented here to generate multiple slave keys (aka site keys) from a single master key for both the offline and online accounts. Among various cryptographic, information-hiding, and non-cryptographic applications needing secrets for various types of key, here are some of the popular applications of secret key: (i) Master key for password vault hiding various keys; (ii) Internet banking; (iii) online stock trading; (iv) insurance; (v) tax; (vi) office, school and home email accounts; (vii) instant messengers; (viii) encrypted files; (ix) database accounts at the office and school; (x) library accounts; and (xi) verification key for credit card. Hence, the impact contribution of multihash

key shall be very high in the aspects of reducing the human memorization burden and system operating costs.

5.4 Acceptable Time Bounds of Multihash Key

The multihash key method and system uses the hash iteration and hash truncation, followed by optional *n*-bit CSPRBG to increase the randomness, as for a basic model of multihash key as in Figure 5.2, to generate slaves keys from a master key and an optional passcode. The master key and hash function shall be at least 2*n* bits. The passcode shall be at least 4 digits or more. The hash iteration applies the key strengthening for a period ranging from 0.2 to 2 seconds, or longer to 10 seconds in some of the variants of multihash key. Hash truncation halves the hash value or message digest. Multihash key supports infinite number of online accounts and limited number of offline accounts depending on the performance of the computer. Examples of online accounts are webmail, login, email, and instant messenger. Examples of offline accounts are encrypted file, public-key certificate, bank ATM card, and software token.

For the present and future times, and in view of the needed number of secret keys for possible amount of offline and online accounts, computer systems with faster processing speed are needed as enabling technologies to accommodate more slave keys of multihash key within the acceptable time bounds.

CHAPTER 6 RESEARCH METHODOLOGY (PART 3): APPLICATIONS OF BIG MEMORIZABLE SECRET & MePKC

6.1 Methods and Systems to Create Big Memorizable Secret

Accordingly, the present invention mainly provides a method to create big memorizable master secret using 2D key, followed by another method to derive multiple slave keys for offline/online accounts from the master key. Every key style of 2D key input method and system can be used individually or mixed as a hybrid combination. The size of big memorizable secret is at least 128 bits. Figure 6.1 illustrates the main and basic operations for the generations and applications of one or more big memorizable secret(s).

6.2 Potential Applications of Available Big Memorizable Secret

With the realization of big memorizable secret, not only the big secret keys of symmetric key cryptosystems of higher security strength like AES-192 and AES-256 can be realized firstly, but memorizable public-key cryptosystem (MePKC) secondly, and other cryptographic, information-hiding, and non-cryptographic applications thirdly, in the information engineering field that need big and yet memorizable secret.

These cryptographic applications include cryptographic schemes like encryption, signature, key exchange, authentication, blind signature, multisignature, group-oriented signature, undeniable signature, threshold signature, fail-stop signature, group signature, proxy signature, signcryption, forward-secure signature, designated-verifier signature, public-key certificate (aka digital certificate), digital timestamping, copy protection, software licensing, digital cheque (aka electronic cheque), electronic cash, electronic voting, BAP (Byzantine Agreement Protocol), electronic commerce, MAC (Message Authentication Code), key escrow, online verification of credit card, multihash signature (Lee, 2009), etc.

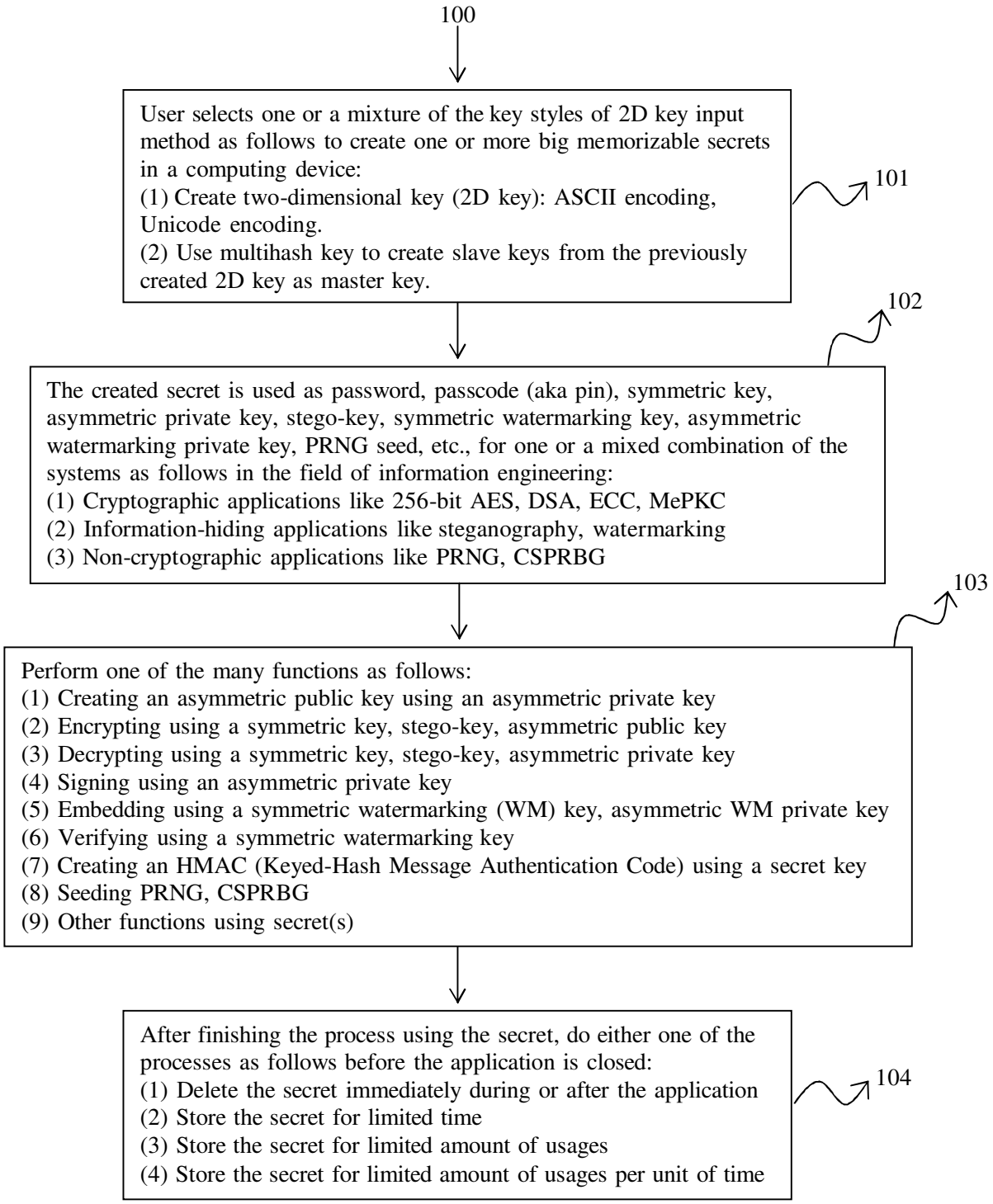


Figure 6.1 Generations and applications of one/more big memorizable secrets

Those information-hiding applications include steganographic and watermarking schemes like stego-key in steganography, secret key in symmetric watermarking, private key in asymmetric watermarking, etc. Meanwhile, the non-cryptographic applications are PRNG (Pseudo-Random Number Generator) and CSPRBG (Cryptographically Secure Pseudo-Random Bit Generator). Hence, there exist lots of needs to have big memorizable secret for lots of cryptographic, information-hiding, and non-cryptographic applications in the field of information engineering, generally, and information security engineering, particularly.

6.3 Main Applications for Symmetric and Asymmetric Key Cryptosystems

With the emergence of 2D key having the styles of mutliline passphrase, crossword, ASCII art / Unicode art, colourful text, and sensitive input sequence, high-entropy key as high as 256 bits is possible. We can now overcome the human factor of memorizability and user interface problem of single-line key field, which have limited the key size to 96 bits or about 100 bits.

Table 6.1 shows the possible dimensions of ASCII-based 2D key for various key sizes of symmetric key cryptosystem. Key strengthening can boost up another 19.5 bits. If Unicode-based 2D key is used, the dimensions of 2D key can be greatly reduced. From Tables 2.3 and 4.1, the settings sufficiency of 2D key input method and system for various key sizes is shown. It can be observed that larger key sizes than 128 bits for cryptographic, information-hiding, and non-cryptographic applications like AES-128, AES-192, AES-256, ECC-256, etc., can be realized by using the 2D key, especially the MePKC using fully memorizable private key.

Table 6.1 Dimensions of 2D key for various symmetric key sizes

Symmetric key size (bits)	80	96	112	128	192	256
Number of ASCII characters	13	15	18	20	30	39
Dimensions of 2D key (ASCII)	3 x 5	3 x 5	3 x 6	4 x 5	5 x 6	5 x 8

For asymmetric key cryptosystem, memorizable public-key cryptosystem (MePKC) can be created. This is possible by using the FFC and ECC with minimum

size of private key at 160 bits. The private key of MePKC is stored in the human brain, and not stored as encrypted, split, and roaming private keys as in the prior arts. This provides mobility, lower cost, higher efficiency, and resistance to dictionary attack and pre-computation attack.

Assuming that the maximum memorizable key size is 256 bits, 256-bit MePKC using FFC and ECC with 128-bit security strength can be realized. It has a protection period of 30 years. If key strengthening is used, 19.5 bits is added, or an increase of 10-bit security, which extends the protection to 50 years. This is very much enough for many practical applications.

A software prototype of this 2D key (Lee, 2006a, 2008i, 2009c, 2010a) with the function of multihash key (Lee, 2007a) has been built up by using the Microsoft Visual Studio (Marshall, 2003). The 2D key can have optional anti-keylogging application software (Log This, No date; McNamara, 2003, pp. 197-202) to achieve higher security during the input. To get a copy of this software, please visit [URL: www.xpreeli.com].

There are other potential applications of 2D key method and system. Firstly, 2D key can be specialized to include only numeric digits or other sets of limitedly encoded characters for devices with limited space like the display and key pad of a bank ATM machine and computerized safety box. Secondly, the display of 2D key can be an LCD display or other display technologies integrated with a computer keyboard having a first partial 2D key optionally visible and a second partial 1D key in hidden mode only to better resist the shoulder-surfing attack.

6.4 Prototyped Applications of Created Big Memorizable Secret(s)

For useful applications of the created big memorizable secret(s) and MePKC, the prototyped applications in software form, that have been built for experimental testing by Kok-Wah Lee the author, include:

(i) method and system to realize memorizable symmetric key the secret till resistance to quantum computer attack;

(ii) method and system to realize encryption scheme of memorizable public-key cryptography (MePKC); and

(iii) method and system to realize signature scheme of memorizable public-key cryptography (MePKC).

6.5 Memorizable Symmetric Key to Resist Quantum Computer Attack

Due to the successful cracking of 56-bit DES (Data Encryption Standard) in the 1990s, stronger symmetric ciphers with larger symmetric key sizes like 80-bit 2TDES, 112-bit 3TDES, as well as 128-, 192-, and 256-bit AES (developed from Rijndael cipher) are introduced to replace the DES.

Blaze, Diffie, Rivest, Schneier, Shimomura, Thompson and Wiener (1996) discussed the minimal key lengths for symmetric ciphers. The NIST (National Institute of Standards and Technology), USA, proposes different protection periods for security through years 2010, 2030, and beyond 2030, for 80, 112, and 128 bits, respectively (E. Barker, W. Barker, Burr, Polk, & Smid, 2007a, 2007b). ECRYPT of European Union (EU) proposes in its technical reports that 80-, 96-, 112-, 128-, and 256-bit security have protection periods of 4 years through year 2010, 10, 20, 30 years, and foreseeable future to be against quantum computer attack, respectively (Gehrmann & Näslund, 2005, 2006, 2007). Nevertheless, conventional methods and systems normally can only realize a key size of 128 bits or less.

Hence, the first application in Section 6.4(i) of the present invention in applying the created big memorizable secret is to realize higher security levels of symmetric ciphers like AES-192 and AES-256. By using the 2D key input method and multihash key as in Figure 6.1 and Table 4.1, it can be observed that the current highest security level of symmetric cipher at 256 bits can be practically realized and achieved using big memorizable 256-bit secret.

Prototypes of application software have been built to experimentally test the applications of big memorizable secret using 2D key and multihash key for symmetric key cryptosystem like AES-128, AES-192, and AES-256.

6.6 Memorizable Public-Key Cryptography (MePKC)

6.6.1 The Proposed MePKC Applications 6.4(ii)-(iii)

The second and third applications 6.4(ii)-(iii) of the present invention in applying the created big memorizable secret are to improve from the token-based public-key cryptography (PKC) to the realization of secret-based PKC using fully memorizable private key, which is named as MePKC (Memorizable Public-Key Cryptography) or MoPKC (Mobile Public-Key Cryptography) here. The main advantages of MePKC are full secret memorizability and mobility convenience. Yet another quite important advantage is that secret-based MePKC can resist some side-channel attacks vulnerable to token-based PKC, such as those attacks over the fully or partially encrypted private key. For illustration of MePKC, please refer to Figure 6.2.

The current lowest key size requirement of asymmetric private key is 160 bits operating in FFC and ECC. From Table 4.1 listing the dimensions of proposed novel 2D key input method and system to create big memorizable secret, a 160-bit secret for 160-bit fully memorizable private key can be supported by a rather small 2D key space. This group of big memorizable secret creation method and system can easily support memorizable private key up to 256 bits at the symmetric bits of security strength of 128 bits and for a protection period of 30 years.

For higher security levels up to 512-bit secret used by 512-bit MePKC, multi-factor multimedia key using software token (Lee, 2008h, 2008l, 2009a) has to be adopted to halve the key size requirement towards a practical realization. Here, the mobility convenience is somehow sacrificed.

The MePKC can be used for major PKC cryptographic applications like encryption and digital signature schemes. Other minor applied cryptographic schemes are key exchange, authentication, blind signature, multisignature, group-oriented signature, undeniable signature, threshold signature, fail-stop signature, group signature, proxy signature, signcryption, forward-secure signature, designated-verifier signature, public-key certificate (digital certificate), digital timestamping, copy protection, software licensing, digital cheque (aka electronic cheque), electronic cash, electronic voting, BAP (Byzantine Agreement Protocol), electronic commerce,

MAC (Message Authentication Code), key escrow, online verification of credit card, multihash signature (Lee, 2009), etc.

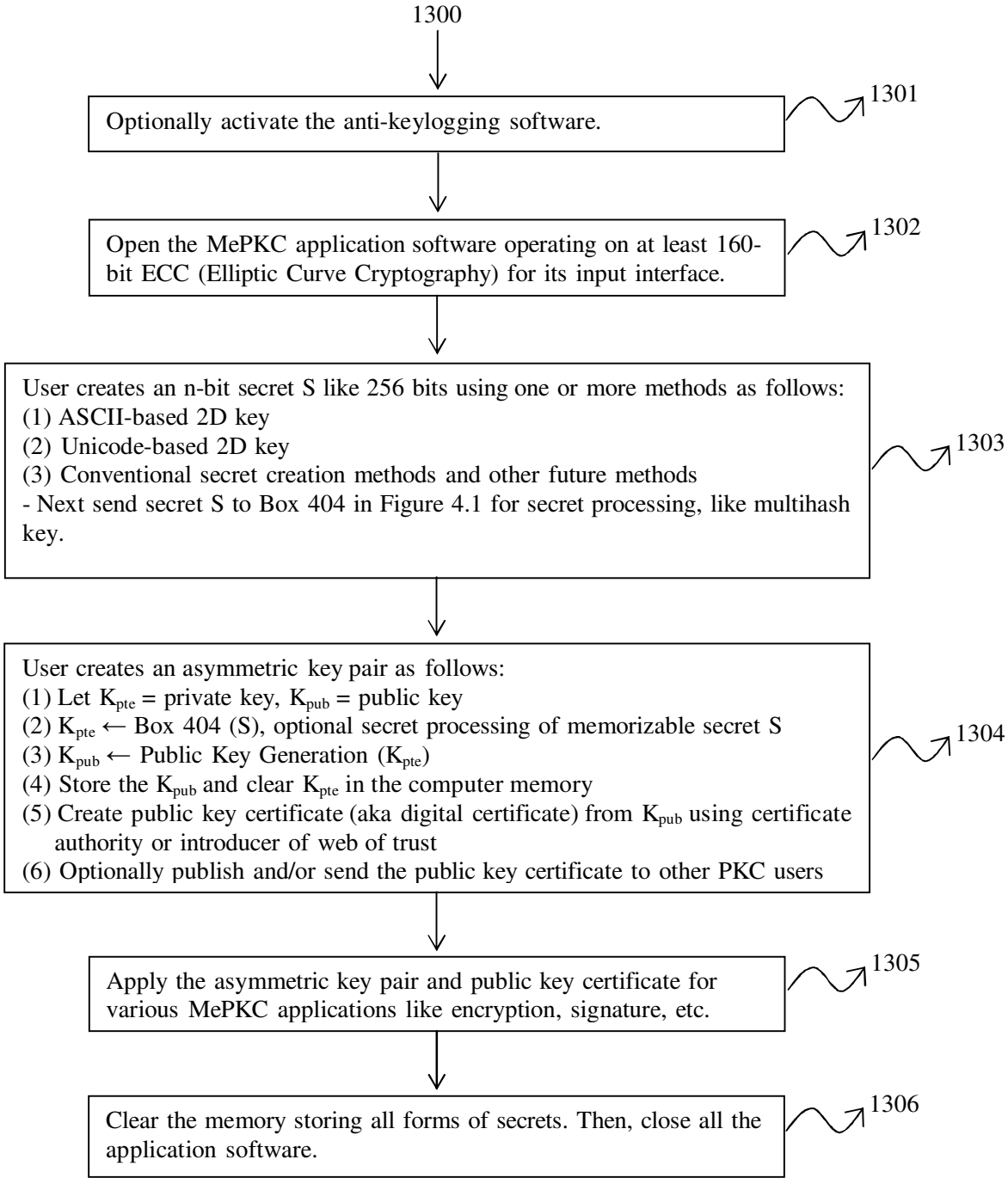


Figure 6.2 Operation of MePKC method and system

The blind signature scheme includes its further applications for electronic cash (aka e-cash, electronic money, e-money, electronic currency, e-currency, digital cash, digital money, digital currency, or scrip), and electronic voting (aka e-voting, electronic election, e-election, electronic poll, e-poll, digital voting, digital election, or digital poll).

Advancement of computing technologies requests for longer key sizes for a fixed protection period. To freeze this unwanted request, key strengthening (aka key stretching) through many rounds of hash iteration, together with hash truncation and a hash function with longer hash value like 768, 1024 bits or more, can be used.

MePKC was extended by Lee (2008h, 2008l, 2009a) there to other novel claimed inventions called multihash signature scheme, and novel innovations of some cryptographic schemes like digital cheque, software licensing, human-computer and human-human authentication via a computer communication network, as well as MePKC digital certificate with multiple public keys for password throttling and ladder authentication.

These MePKC applications are best to be implemented using the ECC (Silverman, 1986; Blake, Seroussi, & Smart, 1999, 2005; Hankerson, Menezes, & Vanstone, 2004, 2005; Zhu & Zhang, 2006). This is because ECC needs a minimum private key size of 160 bits and it has been long time tested for its security strength. Alternatively, depending on further research and evaluation, shorter private key size at equivalent or better bits of security strength can be achieved by using hyperelliptic curve cryptography (HECC) (Pelzl, Wollinger, & Paar, 2004; Cohen & Frey, 2006; Wang & Pei, 2006) and possibly other cryptosystems like torus-based cryptography (TBC) (Rubin & Silverberg, 2003).

For HECC, the genera 2 and 3 have so far been tested to have shorter key size requirement than ECC by twice and thrice. Between them, genus-2 HECC has a higher security without the demand to have a correction factor for its key size. In other words, the correction factor of HECC of genus 2 is 1. As information, genus-3 and genus-4 HECC have a correction factor of 1.05 and 1.286 times of its field, respectively, for the key size to get a larger group order at equivalent bits of security strength. For more information, please refer to an article entitled “High Performance

Arithmetic for Special Hyperelliptic Curve Cryptosystems of Genus Two" by Jan Pelzl, Thomas Wollinger, and Christof Paar (2004).

6.6.2 Selection of ECC Curve to Prototype MePKC Schemes

For second applications 6.4(ii), prototype of application software has been built to experimentally test an example of encryption scheme of MePKC, i.e. 192-bit ECC, by using a software package called Microsoft Visual Studio .NET 2003 (Academic Edition).

For the settings of the 192-bit ECC, a 192-bit pseudo-random curve over prime field (P-192) (NIST, 2006c) has been selected as in Equation (6.1), following paragraphs for parameter definition and initialization, in which it is suitable for both the built prototypes of MePKC encryption scheme and MePKC signature scheme.

$$y^2 \equiv x^3 + ax + b \pmod{p} \tag{6.1}$$

To define the parameters of ECC curve P-192 (NIST, 2006c; Hankerson, Menezes, & Vanstone, 2004, 2005), we have:

- the prime modulus p
- the order n
- the N-bit input seed S to SHA-512 based algorithm, like N = 160, 512
- the output c of the SHA-512 based algorithm
- the coefficient a
- the coefficient b (satisfying $cb^2 \equiv a^3 \pmod{p}$)
- the cofactor h
- the base point x coordinate G_x of point $G(G_x, G_y)$
- the base point y coordinate G_y of point $G(G_x, G_y)$

The integers p and r are given in decimal and hex forms; bit strings and field elements are given in hex form. To initialize the parameters of ECC curve P-192 (NIST, 2006c; Hankerson, Menezes, & Vanstone, 2004, 2005), we have:

P-192: $p = 2^{192} - 2^{64} - 1$, $a = -3_{10}$, $h = 1_{10}$

$p = 6277101735386680763835789423207666416083908700390324961279_{10}$

$n = 6277101735386680763835789423176059013767194773182842284081_{10}$

n = 0x ffffffff ffffffff ffffffff 99def836 146bc9b1 b4d22831

S = 0x 3045ae6f c8422f64 ed579528 d38120ea e12196d5

c = 0x 3099d2bb bfcb2538 542dcd5f b078b6ef 5f3d6fe2 c745de65

b = 0x 64210519 e59c80e7 0fa7e9ab 72243049 feb8deec c146b9b1

G_x = 0x 188da80e b03090f6 7cbf20eb 43a18800 f4ff0afd 82ff1012

G_y = 0x 07192b95 ffc8da78 631011ed 6b24cdd5 73f977a1 1e794811

6.6.3 Encryption Scheme of MePKC

Using a simple ECC encryption scheme (Stallings, 2006), we firstly define parameter as follows:

k_A = user A's private key from a 192-bit secret, where $0 < k_A < n$

P_A = user A's public key

k_B = user B's private key from a 192-bit secret, where $0 < k_B < n$

P_B = user B's public key

z = 192-bit random number, where $0 < z < n$

$P_Z(P_{Zx}, P_{Zy})$ = point of random number z, satisfying $P_z = zG \pmod p$

$P_D(P_{Dx}, P_{Dy})$ = point of random number z, satisfying $P_D = zP_B \pmod p$

E = plaintext of 192-bit symmetric key, where $0 < E < p$

F = ciphertext of 192-bit symmetric key

M = plaintext of message

C = ciphertext of message

To encrypt a plaintext of message M, we then use a hybrid encryption system of symmetric key cryptosystem and asymmetric key cryptosystem. This is because the latter system is 1000 times slower than the former system. Asymmetric key is used to encrypt the symmetric key; whereas symmetric key is used to encrypt the plaintext of message. The encryption stage of MePKC encryption scheme is experimentally tested (Lee & Tan, 2006) according to the pseudocode in Figure 6.3. Meanwhile Figure 6.4 shows the decryption stage of MePKC encryption scheme.

(1.0) User A creates one's public key P_A and send to user B:
(1.1) $P_A \leftarrow k_A G \pmod p$

(2.0) User B creates one's public key P_B and send to user A:
(2.1) $P_B \leftarrow k_B G \pmod p$

(3.0) User A is to send message M to user B:
(3.1) $P_Z \leftarrow zG \pmod p$; $P_D \leftarrow z(k_B G) \pmod p \leftarrow zP_B \pmod p$
(3.2) $F \leftarrow E * P_{Dx} \pmod p$
(3.3) C ← encrypt(M, E), using AES-192.
(3.4) Send P_Z , F, and C to user B.

Figure 6.3 Encryption stage of MePKC encryption scheme (P-192)

(1.0) User B receives P_Z , F, and C from user A.

(2.0) User B decrypts for symmetric key E:
(2.1) $P_D \leftarrow k_B(zG) \pmod p \leftarrow k_B P_Z \pmod p$
(2.2) $F^{-1} \leftarrow$ multiplicativeInverse(F) (mod p)
(2.3) $E \leftarrow P_{Dx} * F^{-1} \pmod p \leftarrow P_{Dx} / F \pmod p$

(3.0) User B decrypts for message M:
(3.1) M ← decrypt(C, E), using AES-192.

Figure 6.4 Decryption stage of MePKC encryption scheme (P-192)

6.6.4 Signature Scheme of MePKC

ECDSA stands for Elliptic Curve Digital Signature Algorithm. Using the ECDSA signature scheme (Hankerson, Menezes, & Vanstone, 2004, 2005), we firstly define parameter as follows:

k_A = user A's private key from a 192-bit secret, where $0 < k_A < n$

P_A = user A's public key

k_B = user B's private key from a 192-bit secret, where $0 < k_B < n$

P_B = user B's public key

z = 192-bit random number, where $0 < z < n$

$P_Z(P_{Zx}, P_{Zy})$ = point of random number z, satisfying $P_z = zG \pmod p$

r, s = 192-bit bitstream, where $0 < r < n$, $0 < s < n$

M = message

e = message digest by hashing message M using hash function like SHA-512

DS = digital signature consisting of (r, s)

(1.0) User A creates one's public key P_A and send to user B:
(1.1) $P_A \leftarrow k_A G \pmod p$

(2.0) User B creates one's public key P_B and send to user A:
(2.1) $P_B \leftarrow k_B G \pmod p$

(3.0) User A is to sign message M:
(3.1) Select randomly z from [1, n-1].
(3.2) $P_Z \leftarrow zG \pmod p$
(3.3) $r \leftarrow P_{Zx} \pmod n$; if r = 0, go back to Step (3.1).
(3.4) e ← Hash(M), using SHA-512 and 192-bit hash truncation from MSB.
(3.5) $z^{-1} \leftarrow$ multiplicativeInverse(z) (mod n)
(3.6) $s \leftarrow z^{-1} * (e + rk_A) \pmod n$; if s = 0, go back to Step (3.1).
(3.7) DS ← (r, s)

(4.0) User A sends message M and digital signature DS(r, s) to user B.

Figure 6.5 Signing stage of MePKC signature scheme (P-192)

Software prototype has also been built and tested for MePKC signature scheme (Lee & Tan, 2006) based on elliptic curve P-192 in Section 6.6.2. Figures 6.5-6.6 shows the signing stage and verification stage of MePKC signature scheme, respectively.

(1.0) User B receives message M and digital signature DS(r, s) from user A.

(2.0) User B verifies the digital signature DS:
(2.1) If r = 0 or r > n-1, reject the signature.
(2.2) If s = 0 or s > n-1, reject the signature.
(2.3) e ← Hash(M), using SHA-512 and 192-bit hash truncation from MSB.
(2.4) s^{-1} ← multiplicativeInverse(s) (mod n)
(2.5) w ← s^{-1} (mod n) ← 1 / s (mod n)
(2.6) u_1 ← ew (mod n); u_2 = rw (mod n)
(2.7) V(V_x , V_y) ← $u_1G + u_2P_A$ (mod p)
(2.8) If V = ∞, i.e. point at infinity or zero point, then reject the signature.
(2.9) v ← V_x (mod n)
(2.10) If v = r, then accept the signature; else, reject the signature.

Figure 6.6 Verification stage of MePKC signature scheme (P-192)

6.7 Other Cryptographic, Information-Hiding, and Non-Cryptographic Applications of Secret beyond 128 bits

Other useful applications of the present invention in applying the created big memorizable secret is various other cryptographic, information-hiding, and non-cryoptographic applications needing a big memorizable secret(s). Interested readers may try to imagine those applications, and then will know that abundant fully big memorizable secret keys are needed, in which 2D key and multihash key can jointly solve this problematic demand.

The other cryptographic applications include various PAKE (Password-Authenticated Key Exchange) like SPEKE (Simple Password Exponential Key Exchange) (Jablon, 2006) and SRP-6 (Secure Remote Password Protocol version 6) (Wu, 2003).

Meanwhile, information-hiding applications (Petitcolas, Anderson, & Kuhn, 1999; Moulin & O'Sullivan, 2003) include stego-key in steganography (Simmons, 1984, 1998; Anderson & Petitcolas, 1998; Cachin, 1998; Mittelholzer, 1999; Fridrich & Goljan, 2004; Fridrich, Goljan, & Soukal, 2004; Lu, 2005), secret key in symmetric watermarking, and private key in asymmetric watermarking (Swanson, Kobayashi, & Tewfik, 1998; Low & Maxemchuk, 1998; Hartung & Kutter, 1999; Mittelholzer, 1999; Mohanty, 1999; Wolfgang, Podilchuk, & Delp, 1999; Eggers, Su, & Girod, 2000; Collberg & Thomborson, 2002; Hachez & Quisquater, 2002; Arnold, Schmucker, & Wolthusen, 2003; Furon, 2005; Furon & Duhamel, 2003; Barni & Bartolini, 2004; Cayre, Fontaine, & Furon, 2005a, 2005b, 2005c; Lu, 2005; Cox, Doërr, & Furon, 2006; Furht & Kirovski, 2006a, 2006b).

Lastly, non-cryptographic applications include seed for PRNG (Pseudo-Random Number Generator) and CSPRBG (Cryptographically Secure Pseudo-Random Bit Generator) (Eastlake, Crocker, & Schiller, 1994; Rukhin, Soto, Nechvatal, Smid, Barker, Leigh, Levenson, Vangel, Banks, Heckert, Dray, & Vo, 2001; Le Quere, 2004; Keller, 2005; Barker & Kelsey, 2007; Campbell & Easter, 2007b) like the Blum-Blum-Shub (BBS) CSPRNG (Mollin, 2007a, p. 508, 2007b).

CHAPTER 7 RESEARCH METHODOLOGY (PART 4): ANTI-HACKING DATA STORAGE USING IMPROVED DIP SWITCH

7.1 Overview

A dual in-line package (DIL/DIP) switch has been modified to collectively link all the poles using a single actuator and called anti-hacking DIP switch. The actuator can be a raised/recessed slide, raised/recessed rocker, or piano-type (aka side/level), selectively switching on or off one/two groups of poles oppositely. A specific inventive application is when a 10/12-way anti-hacking DIP switch is integrated with two modular jack RJ45 sockets and a second storage device preferably via USB connection, a secure data storage resisting the computer hacking in a malicious computer network is created. This new component is simple, cost-effective, and anti-hacking. Yet a novel variant is N_1PST+N_2PST DIP switch with reverse activation.

7.2 Introduction

Hacking or cracking into a computer from a malicious computer network is a great threat to the information security of private and confidential data in this electronic society. History of hacking and cracking can be traced. To resist the hacking and cracking, network settings and firewall software (Ogletree, 2000) are among the available best tools. However, these tools are complicated and not user-friendly to a networking novice like common Internet user. They are only good to network administrator who has undergone training and/or understood the operating manual.

In other words, network settings and firewall software are excellent at the server side but not the client side. Technical difficulty and affordable cost are two main factors discouraging the users to adopt these two anti-hacking approaches effectively. Furthermore, end users normally do not require data sharing via web hosting like server. This indicates that private and confidential data of end users can

actually be partitioned from the data without security concern. For more information on the imperative demand of anti-hacking data storage, please refer to a book excerpt by Burgess and Power (2008) as follows:

"The U.S. Chamber of Commerce estimates that counterfeit and pirated products account for 5 percent to 7 percent of the global economy, and results in the loss of more than 750,000 jobs and approximately $250 billion in sales to the United States alone. … …

The threats of economic espionage and intellectual property (IP) theft are global, stealthy, insidious, and increasingly common. According to the U.S. Commerce Department, IP theft is estimated to top $250 billion annually and also costs the United States approximately 750,000 jobs. The International Chamber of Commerce puts the global fiscal loss at more than $600 billion a year."

In addition to the financial loss of confidential information and business secret, there are cronies of organized crime using the hacked secrets, flash mob approach, and sound snatching to conspire for more serious crimes like to worsen a good human relationship and/or to fasten a cheating human interaction. Married couples may be made divorced. Lovers may be made suspicious between themselves. Relatives, friends, colleagues, and organization members may be made trust-less and negatively emotional. Cheaters may succeed to establish trust, cultivate positively false emotion, and build a dishonest relationship leading to a marriage for sharing or even controlling the power, wealth, reputation, and fame of a single man or woman with good social status. In short, the criminals may cheat for secret, sex, trust, emotion, power, money, and assets.

Beaver (2004) reported that a networked computer without proper firewall (Ogletree, 2000) settings would be hacked within 30 minutes. Yet in the latest news, Markoff (2008) informed that the hacking period dropped to less than 5 minutes after a hacker had operated for 30 seconds to access a prey computer. This reflects how serious and dangerous the current computer communications network security (Stallings, 2000) is in this networked info-computer era.

Identity theft can happen when a hacker copies a prey's computer data as disk image using disk cloning software, and then put the disk image into a second computer and modify, add, delete, etc. on some contents, which can create imitator-type zombie computer and/or infected-type botnet. This imitator-type zombie computer, when connected to the Internet, can fool other prey hackers watching this zombie computer version 2. Of course, if there are any confidential information, business secret, and other intangible assets, in the prey computers, then they shall be considered as disclosed and released to the hackers, or wider to the public domain.

Here, method and device are proposed to secure an anti-hacking data storage for end users. This method uses a new component called anti-hacking DIP switch integrated with two modular jack sockets and a second storage device like hard disk drive (HDD) or USB (Universal Serial Bus) flash drive. Private and confidential data is stored in the second storage device. Anti-hacking DIP switch controls the normal networking mode while it is switched into one direction and anti-hacking mode while it is switched into the opposite direction. This method is simple, cost-effective, and hack-proof. End users can use this method to have anti-hacking working environment without risking the firewall.

7.3 Proposing Improved DIP Switch

For conventional *n*-way nPST (n Poles Single Throw) DIP switch, all the *n* poles are independently switched on or off in parallel with the pin pairs **101** and **102**. A simple structural diagram of a 10-way DIP switch is shown in Figure 7.1. Here, a modified DIP switch called *anti-hacking DIP switch* is innovatively proposed, where all the individual switches of the DIP switch are joined and controlled simultaneously by a transverse slider acting as an actuator in Figure 7.2. Alternative actuators are raised/recessed slide, raised/recessed rocker, or piano-type (aka side/level). When a USB connection is considered, an 8-way anti-hacking DIP switch for Ethernet cable will become 10/12-way, or an extra 2/4-way DIP switch. The slider **103** can be wiped transversely to the pin pairs **104** and **105** to either switch on the networking connection and off the connection of the second storage device, or oppositely. This means DIP switch is 10/12-way nPDT (n Poles Double Throws).

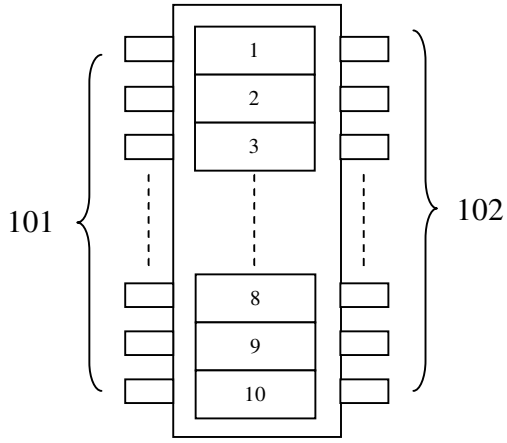


Figure 7.1 Structural diagram of conventional 10-way DIP switch

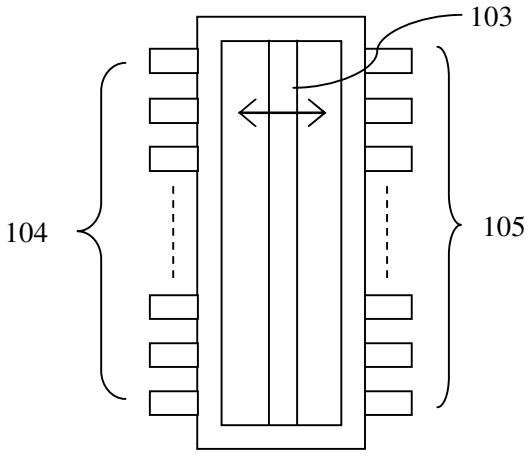


Figure 7.2 Structural diagram of proposed 10/12-way anti-hacking DIP switch

There are two groups of poles in opposite connections: 8-way RJ45/RJ11 networking connection and 2/4-way USB connection. 10Mbps and 100Mbps Ethernet over twisted pair can use 4-way connection, but 1Gbps/1000Mbps Ethernet must use 8-way connection. For USB connection, it can be 4 or 2 ways by saving the power and ground cables. It is then integrated with two RJ45 sockets and two USB sockets to form a simple and cost-effective innovation (Lee, 2008a, 2008b, 2008c).

If Category 5/5e cable defined in ANSI/TIA/EIA-568-A and TIA/EIA-568-B, respectively, is used, the RJ45 socket will be backwards compatible with RJ11 for two running pairs and one running pair, respectively.

7.4 Method and Device to Secure Anti-Hacking Data Storage

Insofar as the anti-hacking DIP switch is specifically designed for a method and device to secure an anti-hacking data storage. An 8/10-way anti-hacking DIP switch is integrated with two modular connector RJ45 sockets to connect or disconnect the networking connection, and two optional USB sockets to oppositely disconnect or connect the second storage device on a PCB (Printed Circuit Board). The integration without USB sockets functioning as an *RJ switch* can be implemented as a wall plate for new installation or as an external interconnection box for old design and inconvenient switch access.

For the end user's computer, a second storage device is needed. This can be either an internal or external hard disk drive (HDD). It can also be a USB flash drive. For external HDD and USB flash drive, they are hot-swappable when USB port is used. For internal HDD of the type of SATA (Serial Advanced Technology Attachment), a switch is needed to control the data connection. This switch called *HDD switch* can be an 8-way DIP switch installed at the back panel of computer with old design or at the front panel of computer with new design. Similarly, the connection of external HDD and USB flash drive via USB port can adopt a 2/4-way switch. This can get rid of the plug-and-play which can cause reliability problem after frequent plugging and unplugging.

Table 7.1 Operating modes of method and device to secure anti-hacking data storage

Operating Mode	Networking Connection	Second Storage Device
Anti-hacking	Disconnected	Connected
Network access	Connected	Disconnected

For real implementation, an RJ switch has been designed and constructed by Kok-Wah Lee, and burnt by Voon-Chet Koo on to a PCB, as an interconnection box from an 8-way DIP switch and two RJ45 sockets. The end user uses a computer connected to an external HDD via USB port. The storage device can also be a USB flash drive. An Ethernet cable links the RJ45 socket of the interconnection box and

computer. Second Ethernet cable links the second RJ45 socket of the interconnection box and the networking wall plate. Clearly, these can be easily understood by any normal end user. The 8-way switch can also be made 10/12-way if the optional USB connection is added. Then, there are two operating modes as in Table 7.1.

For secure anti-hacking operating mode, the actuator is switched to disconnect the networking connection and then connect the second storage device. The end user can create, open, modify, and store one's private and confidential data in the second storage device. When network access is needed, the second storage device is disconnected and then the network is connected. The end user can now surf the Internet and one's data in the second storage device is safe from hacking via the malicious computer network. Once the demand for network access has finished, the end user can switch back to the anti-hacking operating mode to manipulate the private and confidential data. Thus, original plaintext and decrypted ciphertext can be securely stored from virtual hacking at the second storage device.

7.5 Other Forms of Innovation

An innovation of the improved 8-way 8PST DIL switch as in Figures 7.1-7.2 is to become a 10-way 8PST+2PST DIL switch with an actuator activating 8PST and 2PST in opposite direction, where 8PST controls the network connection of RJ-XX and 2PST is extendable to other nPST to control the hot-swappable USB or SATA data/power connection to create an anti-hacking data storage as in Figure 7.3.

As in Figures 7.1-7.2, the 8-way 8PST DIL switch acting as RJ switch for wired Ethernet network can be modified to become 4-way 4PST DIL switch acting as hot-swappable USB switch to control the wireless network connection using the wireless USB network adapter operating on the wireless communication protocols like Bluetooth, Wi-Fi, 3G, WiMAX, etc.

In Figure 7.3, the 10-way 8PST+2PST DIL switch with reverse activation **630** can be modified to have the first 8PST **610** acting as RJ switch or to become 4PST acting as a USB switch for wireless USB network adapter in similarity with Figures 7.1-7.2, and the second 2PST **620** is extendable to other nPST for other types

of data connection, like SATA and USB, to a storage device like HDD and USB flash drive.

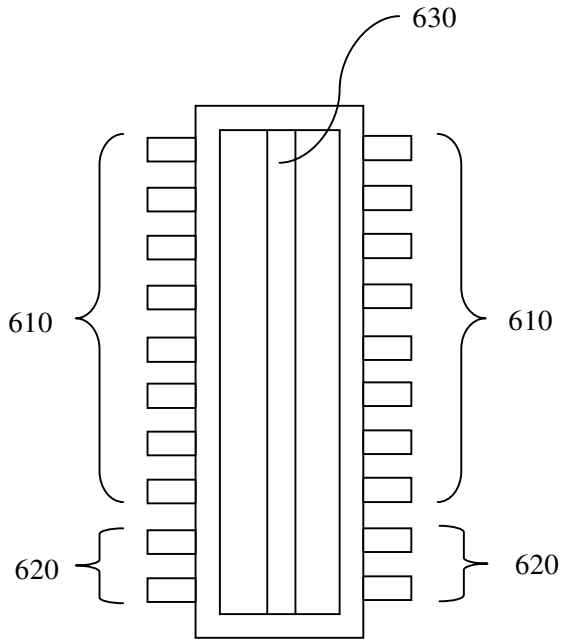


Figure 7.3 Innovated 10-way 8PST+2PST DIL switch activated in opposite direction

The improved DIL switch so far can be other types of switch performing these enhanced functions to create anti-hacking data storage, where they can also switch on or off a few little switches to control the data and power connections like keylock switch, selector switch, pushbutton switch, rocker switch, rotary switch, slide switch, toggle switch, etc., with or without a light indicator of network connection.

There are also some originally novel prototypes for this innovated DIP switch in the forms of layout-design of integrated circuit in Malaysia (Lee, 2005, 2006b, 2007b, 2007c, 2007d, 2007e, 2008d, 2008e, 2008f, 2008g).

CHAPTER 8 RESULTS & DISCUSSIONS

8.1 Overview of Results

For all the four major novel knowledge contributions proposed by Kok-Wah Lee, they can work alone or be integrated to work as a whole as in Figure 8.1.

(1.0) User creates an n-bit big memorizable secret, using 2D key.
(2.0) User feeds the created 2D key as n-bit master key and optionally other parameters into the processing of multihash key to generate multiple n-bit slave keys for offline or online accounts.
(3.0) Each n-bit slave key can be used for any application needing n-bit secret key.
(4.0) Those application types are cryptographic, information hiding, and non-cryptographic types.
(5.0) For PKC using fully memorizable private key directly from 2D key or indirectly, MePKC (Memorizable Public Key Cryptography) is created.
(6.0) Anti-hacking data storage using improved DIP switch is used to securely store the original plaintext and decrypted ciphertext.

Figure 8.1 Overview of the four major novel knowledge contributions

8.2 Two-Dimensional (2D) Key

8.2.1 Discussions: High-Entropy Secret

The advantages of 2D key are good memorizability, high-entropy key, high randomness due to pictorial nature of key styles in 2D space, more references at the user interface to facilitate key input, and resistance to dictionary attack. Even pre-computation attack can be avoided if the 2D secret is used on the platform of MePKC. Moreover, for a long passphrase having many individual units like word, the key input time of 2D key is faster than the single-line key field whenever there is some interrupt and the user has forgotten the input sequence. This is because only that particular sub-unit has to be keyed in again and not the whole secret, such like the secret style of multiline passphrase.

For memory medium, 2D key can be used in paper form and computer form. In term of memory scale, 256 bits can be maximally achieved by most people. The

user's capability in the graphical nature of 2D key decides a person's maximum mnemonic 2D key size. Key styles like crossword, ASCII art, and Unicode art are excellent in resisting guessing attack and dictionary attack. So far there is no feasibly comprehensive dictionary for ASCII art or Unicode art yet on Earth planet. Meanwhile for crossword, the bilingual or multilingual nature and its flexible word architecture can fail the operation of dictionary attack.

Hence, 2D key is unique away from the currently practised 1D (one-dimensional) nature of single-line key/password field, in which 2D key has collectively the features of bigger mnemonic key size and higher randomness. In other words, 2D key is a type of high-entropy secret.

8.2.2 Limitations

Table 4.1 shows the setting sufficiency of 2D key input method. Meanwhile, Table 6.1 shows the possible dimensions of 2D key to have fulfilled the equivalent threshold symmetric key sizes at different security strength. From these two tables, we can see that Unicode-based 2D key can be entered by a user using less number of characters than ASCII-based 2D key, but the current button set of keyboard design for ASCII encoding has limited the input speed of each Unicode character. Thus, regardless of ASCII-based 2D key or Unicode-based 2D key, one of its disadvantages is more time for key input.

For the second weakness, due to non-simultaneous 2D key input upon disturbance, there is possible shoulder-surfing attack from the nearby people or camera, especially the currently popular usage of mobile phones with camera functions. Hence, small 2D key may be used at public areas; whereas bigger and stronger 2D key may be used at private areas, like personal room. This is because the bigger is the 2D key, the longer the time it needs to be entered, and the harder the simultaneity chance it can achieve.

8.2.3 Conclusion

Here, the high-entropy 2D key input method has been proposed. It solves the memorizability problem due to human factor and user interface problem of single-line key/password field. For variability, 2D key has the key styles of multiline passphrase, crossword, ASCII art, Unicode art, colourful text, and sensitive input sequence. The memorizable limit of 96-bit key is increased to 256-bit key, where even the private key is memorizable. This creates 160-bit to 256-bit MePKC with protection period up to 50 years.

8.3 Multihash Key

8.3.1 Discussions: Comparisons

Table 8.1 compares various key management tools with multihash key from the aspects of usability, security, and possible implementation. A lot of comparisons are attributed by Yee and Sitaker (2006) on Passpet. New features used for comparisons are applicability to offline and online accounts, integrated usages together with other key management tools and possible implementations. It is important to note here that multihash key can be used together with Passpet to earn "Yes" for items [I.7-I.9] under the security features in Table 8.1.

Multihash key can be used for both offline and online accounts. Possible implementations are stand-alone application and browser extension. These are simple interfaces to input a password or key with unique key images for multiple accounts. Memorizability is improved since there is only one secret for various login accounts.

Server is not used and hence there is no central authority. There are no single point of failure and high cost of integration. It is mobile and there is no encrypted storage of site keys. Since there is no integration, multihash key can be used for any existing computer systems.

8.3.2 Discussions: Suitable Time Bounds

The passcode is optional to be remembered by a user because it can be converted to be an 8-bit password supplement in one of the two methods of key strengthening (Manber, 1996; Abadi, Lomas, & Needham, 1997, 2000). Master key

is the password, and when it is combined with the password supplement, they form the full password. Another key strengthening method is also called key stretching, which uses a large amount of hash iterations (Kelsey, Schneier, Hall, & Wagner, 1997).

Table 8.1 Comparisons of key management tools

Features\Key management tools	Plain browser	Password autofill	Password safe	Windows live ID	LPWA	HP site password	CPG	Password multiplier	SPP	Pwd Hash	Passpet	Multihash key
Usability												
1. Make logging in more convenient	No	Yes	No	Yes	Yes	No	?	Yes	?	No	Yes	?
2. Work with existing websites	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
3. Allow site-by-site migration to tool	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes
4. Change individual site keys	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes	–	Yes	Yes
5. Log in from other computers	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
6. Only need to memorize one secret	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	–	Yes	Yes
7. Enable changing the master secret	–	–	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes
8. Applicability to offline accounts	–	–	Yes	No	No	No	No	No	No	No	No	Yes
9. Applicability to online accounts	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
10. Integrate usages together with other tools	–	–	Yes	No	No	Yes	No	No	No	No	No	Yes
Security												
1. Unique key for each account	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
2. Resist offline dictionary attacks	No	No	No	No	No	No	No	Yes	No	No	Yes	Yes
3. Adapt to increasing CPU power	No	No	No	No	No	No	No	Yes	No	No	Yes	Yes
4. Avoid storing keys	Yes	No	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
5. Avoid a single central authority	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes
6. Resist phishing by fake login forms	No	No	No	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes
7. Resist mimicry of browser UI	No	No	No	No	No	No	No	No	No	No	Yes	No
8. Help the user identify websites	No	No	No	No	No	No	No	No	No	No	Yes	No
9. Stop entering secrets in webpages	No	No	No	No	No	Yes	?	Yes	?	No	Yes	?
Possible implementation												
1. Stand-alone application	No	No	Yes	No	No	Yes	No	Yes	Yes	Yes	No	Yes
2. Single sign-on server	No	No	No	Yes	Yes	No	Yes	No	No	No	No	No
3. Browser extension	Yes	Yes	No	No	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

?: Unknown situation depending on implementation

The variant of SHA-2, which is SHA-512, is used in the key hashing and key strengthening. This is because there are possible collision attacks to MD5 and SHA-1.

The hash truncation creates a 256-bit hash as site key. The unused truncated bit creates a 128-bit security strength (256/2=128) preventing the compromised site keys at the higher security level from revealing the site keys at the lower security level. The passcode also has this feature but is very much less powerful.

For the experimental data of lower bound b_L and upper bound b_H of some computer systems, there are reported as follows. For instance, for the first computer system of desktop PC [Example 1: Pentium II 266MHz, 192MB RAM, running on Windows XP Professional Edition SP1], the lower and upper bounds for 1-second hash iteration, as in Figure 5.1, are 7600 and 8200, respectively. In other words, the first computer system can only support 20 offline accounts for a security level partitioning of 8 bits or 2^8.

Yet in the second computer system of desktop PC [Example 2: Pentium IV 1.8GHz, 512MB RAM, running on Windows XP Home Edition (version 2002) SP2], the lower and upper bounds for 1-second hash iteration are 39,400 and 41,700 respectively. For this specification, the third computer system can support 100 offline accounts for a security level partitioning of 8 bits or 2^8.

Yet in the third computer system of laptop PC [Example 3: Centrino Duo 1.66GHz, 1.5GB RAM, running on Windows XP Home Edition], the lower and upper bounds for 1-second hash iteration are 81,700 and 93,700 respectively. For this specification, the second computer system can support 256 offline accounts for a security level partitioning of 8 bits or 2^8.

These three computer systems, together with other four, are summarized into Table 8.2. The fourth computer system is a desktop PC [Example 4: AMD Athlon 64 Processor 3800+, 2.40GHz, 1GB RAM, running on Windows 7 Enterprise Edition (version 2009) (32-bit OS)]. The fifth computer system is a desktop PC [Example 5: Intel Pentium D (Dual Core) 2.80+2.79GHz, (512MB or 1GB) RAM, running on Windows XP Professional Edition (version 2002) SP3]. The sixth computer system is a desktop PC [Example 6: Intel Pentium Core2Duo CPU E4600, 2.40+2.39GHz, 3.48/4GB RAM, running on Windows XP Professional Edition (version 2002) SP3]. The seventh computer system is a desktop PC [Example 7: Intel Core i3 2x2.93GHz, 4GB RAM, running on Windows XP Home Edition (version 2002) SP2].

Table 8.2 One-second time bounds of several computer systems

No.	CPU	Lower 1-Second Time Bound (loop)	Upper 1-Second Time Bound (loop)	Range of Time Bound (loop)
1	Intel Pentium II 266MHz	7,600	8,200	600
2	Intel Pentium IV 1.8GHz	39,400	41,700	2,300
3	Intel Centrino Duo 1.66GHz	81,700	93,700	12,000
4	AMD Athlon 64 Processor 3800+ 2.40GHz	69,900	77,300	7,400
5	Intel Pentium D (Dual Core) 2.80+2.79GHz	78,200	87,000	8,800
6	Intel Pentium Core2Duo CPU E4600 2.40+2.39GHz	69,000	76,000	7,000
7	Intel Core i3 2x2.93GHz	185,300	205,500	20,200

Using the proposed settings, the key strengthening has an access time from 0.2 second to 2 seconds. This is an efficient range of acceptable login processing time. It can be calibrated to be parallel with the advances in computer technologies for new releases of multihash key. Moore's Law is a good rule to judge the calibration, which is about one bit faster for every two years.

Key hashing and key strengthening are also good techniques to resist offline and online dictionary attacks as well as pre-computation attacks. To prevent phishing and spoofing attacks, multihash key can either be used together with other anti-phising tool like petname system and Passpet, or include domain name URL in its key hashing. Malicious server attack is also prevented as different accounts have unique passwords. For homograph attack due to visually similar Unicode graphic symbols, the implementation of multihash key shall support the Unicode characters.

Up to here, the basic model of multihash key can support almost infinite number of online account. Meanwhile, the number of supported offline account by multihash key is given by Equation (8.1). From Figure 5.2, the security level x can be

increased up to the maximum of hash iteration number j_{max}. Also, hash functions beyond 512 bits like 768 and 1024 bits may be needed.

$$S_{AC0} = x \tag{8.1}$$

8.3.3 Limitations

Multihash key can be implemented as a stand-alone application with no change of setting at the server side. However, it is vulnerable to password file compromise attacks and message log file attacks. Nevertheless, domino effect of password reuse can be avoided. To get rid of password file compromise attacks and message log file attacks, some countermeasures (Gouda, Liu, Leung, & Alam, 2005) can be adopted by changing the settings of authentication approach at client and server sides.

Acting as a stand-alone application, multihash key requires a user to perform extra steps. These steps are creating a key, copying, and pasting it to a login prompted textbox. The user also needs to remember the security level of an account, an at least 128-bit master key, and a numeric 4-digit passcode. These cause the solution to be not user-friendly.

To facilitate the application, multihash key has to be integrated into the user interface of each authentication application. Therefore, the item [I.1] of usability in Table 8.1 about convenient logging in depends on implementation.

For security level, it can be jotted into a notebook in plaintext form because it is not an essential secret. Alternatively, for online account, the user can be reminded about the security level whenever the user sends the username to the server. This allows an attacker to reduce the number of hash testing by 20 times, or 4.32 bits ($=\log_2 20$).

For numeric 4-digit passcode, it gives an extra security of 13.29 bits ($=\log_2 10\,000$) and is not an essential secret. This passcode can be made constant for user with poor memory. For user who can remember 128-bit master key, 4-digit passcode and security level, the effective security strength is 145.61 bits. For user

who can remember only the 128-bit master key, its security strength is 128 bits. Hence, security can be compensated for better usability.

Using multihash key, limited number of multiple offline and online accounts can be supported as compared to the almost infinite number of online accounts for LPWA, HP Site Password, CPG, Password Multiplier, SPP, PwdHash, and Passpet. For more accounts, faster computer system is needed to have larger range of lower to upper 1-second time bound. Or else, the partition between any two security levels has to be reduced.

8.3.4 Conclusion

The proposed invention of multihash key requires users to remember a master key and passcode to generate unique key hashes (aka site keys, slave keys) for multiple accounts. For security level, username, and domain name of a specific account, users can choose to write them down somewhere as they are not critical secrets. This is a balance between the usability and security.

Multihash key can be used for offline and online accounts, where existing similar key management tools without encrypted site key storage can only be applied to online accounts. It is hoped that this proposal can release the human memory burden on required passwords or keys for various types of increasing accounts. To have better resistance to phishing and spoofing attacks, try to use multihash key together with an anti-phishing tool like petname system and Passpet.

8.4 MePKC & Its Applications

8.4.1 Discussions: Enablement of Amazing Functions

Since the Diffie and Hellman's proposal (1976), PKC (Public Key Cryptography) has become a dream in public domain. Then the RSA of IFC (Integer Factorization Cryptography) (Rivest, Shamir, & Adleman, 1978, 1983) practically realizes the implementation of PKC for encryption scheme and digital signature scheme. Nevertheless, for about 30 years, the secure storage of private key at sufficient key size has been a long lasting open hard problem. The current prior arts

of private key storage are encrypted private key, split private key, and roaming private key. Their common feature, that there is no capable technique to create fully memorizable private key, has greatly constrained the popularity of public key certificate in particular, and the widespread of PKC applications in general.

Mathematics and science with theory only and without any application can hardly stimulate a person's interest. For instance, mathematics is the queen of science, and number theory is the queen of mathematics. However, without the widespread applications of cryptography and computing, number theory would not have become a chapter in the further mathematics subject at pre-university (pre-U) level, like STPM in Malaysia (equivalent with Advanced Level (A-Level) in UK). It is because of the applications of knowledge, like mathematics and science, that humans have technologies later.

Here, 2D key has enabled possible high-entropy private key, which is big, memorizable, and yet random. On the other hand, multihash key has solved the technical and legal problems to have different asymmetric key pairs for different PKC schemes. Gathering both the forces of 2D key and multihash key, a big secret from 2D key as the master key can generate multiple slave keys. Either the 2D key directly, or the slave keys indirectly, have solved the open hard problem of fully memorizable private key. In other words in term of authentication factor, "what you know" like secret can begin dominating the technology of private key storage, by replacing the currently dominant authentication factor "what you have" like token or encrypted ciphertext.

Encryption scheme and signature scheme are the most common applications of PKC. Using Microsoft Visual Basic and Microsoft Visual C++ of Microsoft Visual Studio .NET 2003 (Academic Edition), Kok-Wah Lee has built prototypes of 192-bit MePKC encryption scheme and signature scheme for experiment testing (Lee & Tan, 2006), based on the works of:

(i) Kok-Wah Lee for ECC functions, multiplicative inverse function, data type conversion, and GUI in Microsoft Windows environment;

(ii) multiplicative inverse function from a book by Menezes, Oorschot, and Vanstone (1996);

(iii) ECC functions from a few books (Blake, Seroussi, & Smart, 1999, 2005; Stallings, 2006);

(iv) SHA-512 function from toolbox of Microsoft Visual C++ 2003; and

(v) Alan Wee-Chiat Tan for programming the big number class in C++ language by sourcing the ideas of data type and arithmetic of school book from Kok-Wah Lee.

Coming to Microsoft Visual Studio 2010, the class of big integer arithmetic (aka big number, arbitrary precision arithmetic) has now been included and provided. Thus, one can have more efficient and faster computations of big number, without inventing the wheels again.

Other MePKC applications, that can be imagined for proof of concept, can be referred at Sections 6.2 and 6.6.1. They may or even can collectively solve some potentially critical social problems on Earth planet now in chain effect as follows:

(i) Materials chain: Computer system as multi-purpose machine > electronic world > less demand for materials > less paper and more conserved jungle; less metal and more preserved ore supply > friendly Earth surface environment > green Earth.

(ii) Residence chain: Computer communication network > Internet > online service providers > de-urbanization of population > de-centralization of water supply > less wasted clean water > more supply variety in terms of quality and quantity to suburban and village areas > friendly human living environment > green Earth.

(iii) Equipment chain: Recyclable materials to make computer? (i.e. an open problem) > computer system as multi-purpose machine > replacing other tools, machines, and equipment > nano-electronics > less space demand > more comfortable human population > friendly chemical environment > green Earth.

(iv) Communications chain: Electronic communication and form processing > less transportation > less demand of petroleum > more efficient usage of electricity power > less energy demand > friendly climate environment > green Earth.

For the world summit conferences in the recent years, climate change is the main topic. From experts, they claim that upon an increase of 2^0C (or 2 Kelvins) in temperature relative to the Earth average temperature in year 1900, then the Earth planet will fall into a positive feedback loop to keep on warming up the Earth planet. To prevent this event from happening, the present humans have to take immediate measures.

8.4.2 Limitations

For ASCII-based 2D key, the maximum key size of big secret for normal humans is 256 bits, where up to 256-bit MePKC can be realized and applied. To go until 512-bit MePKC, Unicode-based 2D key is needed. However, the present keyboard is designed for ASCII encoding, and it is not efficient to enter Unicode characters.

During the input of 2D key, especially when it is really big, then a user may need to view the 2D key in plaintext form for the whole entry process. For small 2D key, the 2D key remaining in the hidden form of ciphertext can easily be ensured. Thus, shoulder-surfing attack and hacking attack exist for big 2D key.

Shoulder-surfing attack can be avoided when big 2D key is used only at private areas like personal office, personal home, etc. Hacking attack can be stopped by firstly disconnecting the network access, before the input of big 2D key, and upon finishing entering the 2D key, then connect back to the network like Internet. We can adopt this approach by applying the anti-hacking data storage using improved DIP switch.

Elliptic curve arithmetic is not an easy subject, but very difficult to understand. Thus, this subject may have hindered the progress and harbinger of MePKC and its applications.

8.4.3 Conclusion

MePKC and its applications can stretch from individual works, to small group works, to big group works, or even to super big group works. This can happen

depending on the human's needs for functions in the public key cryptography (PKC) to live in the electronic communications world.

PKC is a way of secure communication. If one were at a university, one can observe the existence of some essential buildings like classroom for learning, library for book reading, hostel for accommodation, restaurant for food and beverage, bus stop and car parks for transportation, bank for financial services, and post office for mail communications and package delivery. There even exists an idiom saying that "Stamp collection is a hobby of kings, and a king of hobbies." as a reminder on the importance of message communications. In battles and wars, the military army is hence to attack, destroy, or capture the enemy's communication stations first. Thus, communications is an imperative, urgent, or important element in human life.

"How to communicate more safely and efficiently in the electronic networked world?" is the main question to be answered by MePKC and its applications in this book. Till here, in this networked info-computer era, do you think that current human societies need computer hardware, computer software, communications network, Internet, multimedia informative contents, cryptography for secure communications, public key cryptography, and MePKC and its applications? Do they in great needs? Do they in immediate needs also? Otherwise, how to conserve a green Earth planet, in view of the current human population at about 7 billion in year 2011?

8.5 Anti-Hacking Data Storage Using Improved DIP Switch

8.5.1 Discussions: Costs and Reliability

The current cost of a DIL switch in Malaysia ranges from MYR$3.88 to MYR$46.77 depending on the contact ratings of voltage and current, and operating life (Farnell, 2007). The FOREX (Foreign Exchange) of USD$1.00 was about MYR$3.50 in September 2007 and October 2008. Mass purchase over 500 pieces can reduce the unit price of DIL switch to MYR$2.56. Subsequently, it can be claimed that the added manufacturing cost is low and yet the added value of anti-hacking data storage is high. As at 26 April 2011, in Malaysia USD$1.00 would have MYR$2.9880.

The voltage and current of applied DIP switch will depend on the power over the Ethernet cable (i.e. PoE (Power over Ethernet), PoL (Power over LAN) or Inline Power), phone cable, and USB connection. Supplying power over Ethernet is strongly recommended to follow the IEEE Standard. Clause 33 of "IEEE 802.3-2005 - Section Two" (LAN/MAN Standards Committee, 2005) provides 48 volts DC over two of the four available pairs on a Cat. 3 / Cat. 5 cable with a maximum current of 400 mA for a maximum load power of 15.4 Watts.

For the Ethernet cable over LAN in Malaysia, it is normally Cat. 5 T568B. Contact rating of phone cable for network usage is below the contact rating of Ethernet cable. If USB power cables travel through the DIP switch, then it is 4 ways and the contact rating is 5.25 V DC and 500 mA. Otherwise, it needs 2 ways and the contact rating of USB data cables is below 2.8 V and 20 mA for high speed USB 2.0.

The reliability (aka operating life or service life) of DIP switch ranges from 1,000 to 35,000 operations. The death of DIP switch depends on the change of contact resistance and the mechanical wear out of the actuator. It is expected that the improvements by Lin (1999) and Tai (2001) can further increased the operating life of DIP switch in parallel with the reduction of manufacturing materials, weight, and cost. It is a question on the balance of costs and reliability.

This innovation is expected to be broadly used in the office environment, where there exists a lot of private and confidential data. If the anti-hacking operating mode and network access operating mode are activated once a day for five times per week, then the DIP switch can last for 3.85 years for the DIP switch with operating life of 1,000 operations. The contact ratings, operating life, and cost of DIP switch are closely correlated. Survey and research are needed for optimum manufacturing design and supply chain management.

Yet another potentially broad application for men with good social status and women with good conditions, this anti-hacking data storage is also critical to protect their human interaction network, daily itinerary, future plans, and financial accounts from being maliciously conspired by the cronies of organized crime by using the hacked secrets, flash mob approach, and sound snatching.

8.5.2 Limitations

There exists a possible loophole for anti-hacking DIP switch, where a skilful hacker can write spyware and send it to infect the first HDD of a networked computer during the network access operating mode. Then, the spyware is to copy the targeted original plaintext or decrypted ciphertext from the secure second storage device to the first hard disk drive during the anti-hacking operating mode. When back to the network access operating mode, the spyware automatically sends or the hacker hacks to get the duplicated secret files.

In fact, this loophole is normally from an advanced hacker to have done so. Bait can be prepared to catch this type of hackers, but cooperation with the network services providers is needed. To get rid of the assistance of network services providers, or the network administrator of the network services provider is the malicious person, then partially true sensitive information or unique secrets have to be prepared in a bait computer to identity the hacker's human networks.

This problem can also be avoided if the software architect of the OS like Microsoft Windows, Linux, and Apple Macintosh can cooperate and collaborate with the computer hardware architect to plant special local commands to execute, read, and write for a specially located storage device or computer port. For instance, a simple case is like the copying process from the secure second storage device to the first HDD can only be manually done via the keyboard command. In another case, the copying process may choose to ask for a password as pre-requisite first.

To avoid another type of advanced hacker to do recovery of deleted file from the electronic storage devices like hard disk drive or flash disk drive, file shredder software can be used. So, for this anti-hacking method, system, and device, we can resist a big percentage of amateurish hackers using hacking tools designed by other expert hackers.

To qualify for advanced hacker to break into this simple and cost effective method, the hacker has to know advanced computer programming language like C/C++ language and the secrets of common operating systems (OS) like Microsoft Windows. For some geniuses, they prefer to use Linux OS to do personalization. For instance, the advanced hacker has to know the network address of prey computer, file

location, file name, OS architecture, access time of isolated data storage device, online time of computer system, and anonymously safe IP address to receive the duplicated secret file to program one's hacking tools like spyware to break into this proposed simple anti-hacking method and system. To resist this type of advanced hacker using personalized spyware, the secret file can be password protected by 2D key the big secret directly, or a slave key of multihash key indirectly.

8.5.3 Conclusion

Unless there is an advanced hacker who can interpret the weak electromagnetic radiation across the anti-hacking DIP switch, this proposed method and device for securing an anti-hacking data storage can be claimed to be fully resisting the hacking attacks. It is a simple integration consisting of an improved DIP switch, two RJ45 sockets, and two optional USB sockets. The proposed switch adds little manufacturing costs but highly added values, which may be a 10-way switch for a RJ45/RJ11 and a USB connection. This anti-hacking method and device is simple, cost-effective, and may even be hack-proof when cooperation of computer hardware architect and software architect has been achieved.

CHAPTER 9 CONCLUSIONS

9.1 Concise Summary

In a nutshell, this doctoral research project has contributed a lot of originally novel knowledge contribution in the forms of methods, systems, and devices in the fields of information engineering, generally, and security engineering, particularly. Contribution impact by referring to the applications of research results for public usages is highly recommended in the operational direction of this project.

Firstly, a method to create big and yet memorizable secrets called two dimensional (2D) key has been invented. To cater for the demands of multiple unique secrets to support various offline and online accounts, the multihash key using the hash iteration and hash truncation is then proposed.

Later, we have applications of big secret(s), like the important MePKC (Memorizable Public-Key Cryptography). MePKC is realized by using the ECC (Elliptic Curve Cryptography). Then, to protect the original plaintext and decrypted ciphertext from hacking, anti-hacking data storage using improved DIP switch is designed.

9.2 Suggestions for Future Research

While reading the recommended supporting reading materials for this research project, readers may also consider developing any of the suggested research topics as discussed in this Section 9.2.

9.2.1 512-Bit Multihash Key Needs Hash Function beyond 1024 Bits

So far the popular and security intensively tested hash function is SHA (Secure Hash Algorithm) family. The longest message digest of this SHA is SHA-512 of SHA-2 with 512 bits. This has limited the application of multihash key to 256-bit security for symmetric key and 128-bit security with 30-year protection for asymmetric private key. To achieve the higher security strength at 256 bits of

symmetric key strength for 512-bit asymmetric private key, multihash key needs to use 1024-bit hash function to generate 512-bit final slave key.

For 1024-bit hash function, there exists a scalable polymorphic hash function (Roellgen, No date) to achieve this kind of message digest. Nevertheless, its security strength is not well tested by the peer researchers in information security. Therefore, while NIST is in the process of opening a website to accept the recommendation of SHA-3, even though its maximum hash value requirement is 512 bits, related researchers have to prepare themselves to go for a longer message digest up to 1024 bits to realize the 256-bit to 512-bit MePKC (Memorizable Public-Key Cryptography).

9.2.2 MePKC Extension to Other Non-Conventional Cryptographic Schemes

In this thesis, the MePKC has been applied for encryption scheme and digital signature scheme. Other possible extensions are authentication, BAP (Byzantine Agreement Protocol), electronic commerce, and digital timestamping.

Besides these conventional cryptographic schemes, interested researchers may apply MePKC for other non-conventional cryptographic schemes like key exchange, blind signature, multisignature, group-oriented signature, undeniable signature, threshold signature, fail-stop signature, group signature, proxy signature, signcryption, forward-secure signature, designated-verifier signature, copy protection, electronic cash, electronic voting, MAC (Message Authentication Code), key escrow, online verification of credit card, etc. Others include digital cheque (aka electronic cheque), software licensing, public-key certificate of public-key infrastructure (PKI), and multihash signature.

The blind signature scheme includes its further applications for electronic cash (aka e-cash, electronic money, e-money, electronic currency, e-currency, digital cash, digital money, digital currency, or scrip), and electronic voting (aka e-voting, electronic election, e-election, electronic poll, e-poll, digital voting, digital election, or digital poll).

9.2.3 Big Secret(s) for Information-Hiding and Non-Cryptographic Applications

In addition to the big secret(s) applications for cryptographic schemes, Section 6.7 has listed other applications of big secret(s) including the information hiding and non-cryptographic applications. The information-hiding applications include steganography, symmetric watermarking, and asymmetric watermarking. The non-cryptographic applications are to be the seeds of PRNG (Pseudo-Random Number Generator) and CSPRNG (Cryptographically Secure PRNG).

Hence, there are lots of spacious rooms to evaluate the key sizes and corresponding bits of strength of these other applications of big secret(s). It is highly expected for the existence of some literatures about their practically secure key lengths and protection periods like the cryptographic schemes ("Cryptographic Key Length Recommendation," No date; E. Barker, W. Barker, Burr, Polk, & Smid, 2007a, 2007b; Gehrmann & Näslund, 2005, 2006, 2007).

9.2.4 Safety Box Using Computerized Lock

For safety box using computerized lock (Domenicone, 2000), its key pad is purely numeric and the display panel is single-line. The short-term memory limits of digits have been studied by Miller (1956) to be an average of 7 items plus or minus 2 (7 ± 2) (Jones, 2002; Doumont, 2002), and further studies show that they depends on languages (Jones, 2002) in general and phonological short-term memory of 2-second period (Baddeley, Thomson, & Buchanan, 1975) in particular. It is 9.9 digits in Chinese language (Hoosain & Salili, 1988) and 5.8 digits in Welsh language (Ellis & Hennelly, 1980).

In other words, for single-line numeric passcode of this type of safety box, a user using English, Chinese, or Welsh language will have a passcode with average entropy of 23.25, 32.89, or 19.27 bits, respectively. The strength of these key lengths is insecure whenever a brute force attack can be launched towards the safety box.

Therefore, 2-dimensional (2D) key is highly appreciated to be applied into the safety box using computerized lock. For the key pad, it can remain to be purely numeric in decimal digits or enlarged to become in hexadecimal digits.

9.2.5 Provable Security Studies

The only researcher, who is Kok-Wah Lee @ Xpree Jinhua Li, contributing to the originally novel knowledge in this book, is educated in electrical engineering in general and computer communications in particular. Hence, a lot of the proofs of the inventions and innovations here are based on building up engineering prototypes. Consequently, researchers in provable security, who are also mathematicians, are expected to analyze thoroughly the security strength and loopholes of the algorithms, methods, systems, devices, and apparatuses in security engineering in this thesis.

The initial name of "provable security" is more accurate as "reduction-based security", which has explicitly been telling the feature of "experimental then analytic proof" for this information security field by depending on the available cryptographic primitives like AES, RSA, ECC, etc.

9.2.6 Statistical Surveys for Various Security Schemes

Besides the provable security research over the inventions and innovations proposed here, researchers in statistics can also consider conducting surveys like some surveys (Adams & Sasse, 1999; Schneier, 2006; Florencio & Herley, 2007) to know about the minimum, mean, maximum, and median key lengths of those applications of method and system to create big and yet memorizable secret as proposed here. Similar statistical surveys can also be carried out for multihash key to know the statistical values of master keys and slave keys.

9.3 Future Development of Keys the Secret

These keys the secret need good generation methods (Scalet, 2005) and key management (Fumy & Landrock, 1993; Beach, 2001; Witty, 2001). Wailgum (2008)

questioned on whether there were too many passwords or humans were lacking of memory power. In term of memory, there are two forms: Recognition-based and recall-based. Weinshall and Kirkpatrick (2004) presented those recall-based passwords. Bill Gates with Microsoft has once claimed the ending of the passwords (Allan, 2004; Kotadia, 2004; Fried & Evers, 2006).

Subsequently, there are introductions of some password alternatives like Information Card, Windows CardSpace (Wilson, 2008), Higgins Project, OpenID, Identity Metasystem (Jones, 2005; Cameron & Jones, 2006), Identity Selector, digital identity (Cameron, 2005; Cavoukian, 2006), Authorization Certificate, Extended Validation Certificate, etc.

Furnell (2005) analyzed whether human could get rid of passwords and concluded that passwords could not be replaced. Here, if the inventions and innovations on big secret(s) creation methods and their applications are adopted, especially MePKC (Memorizable Public-Key Cryptography), the complicatedly mentioned password alternatives may be made simpler or at best be avoided. More literatures on password are available at PasswordResearch.com (No date) website [URL: www.passwordresearch.com].

For security of asymmetric key cryptosystems, the mathematical hard problems depend on the researchers' creativity and innovation as well as the computing technologies to crack them. For example, the cryptanalytic attacks like Wiener (1990) and so on, that can be discovered in the future, may request for longer asymmetric key sizes and/or other mathematical hard problems. Challenges with awards offered by the PKC services providers to crack certain PKC with certain key sizes are always there for the public to attempt.

Anyway, the practically secure key sizes for symmetric and asymmetric key cryptosystems at different protection periods are always under the regular evaluations by a lot of researchers (Williams, 2002). Website of KeyLength.com [URL: www.keylength.com] ("Cryptographic Key Length Recommendation," No date) is a collection database for lots of documentations on these practically secure key sizes for various applications in security engineering, particularly, and information engineering, generally.

9.4 Conclusions

To emphasize again on the imperative aim of this research project, here is the last paragraph.

Let's create and maintain a networked info-computer age for a more paperless, trip-less, petroleum-less, and environment-friendly human society by having safer multipartite electronic computer communications as from the original and novel knowledge contribution of this research project.

APPENDIX A WRITING SYSTEMS OF THE WORLD

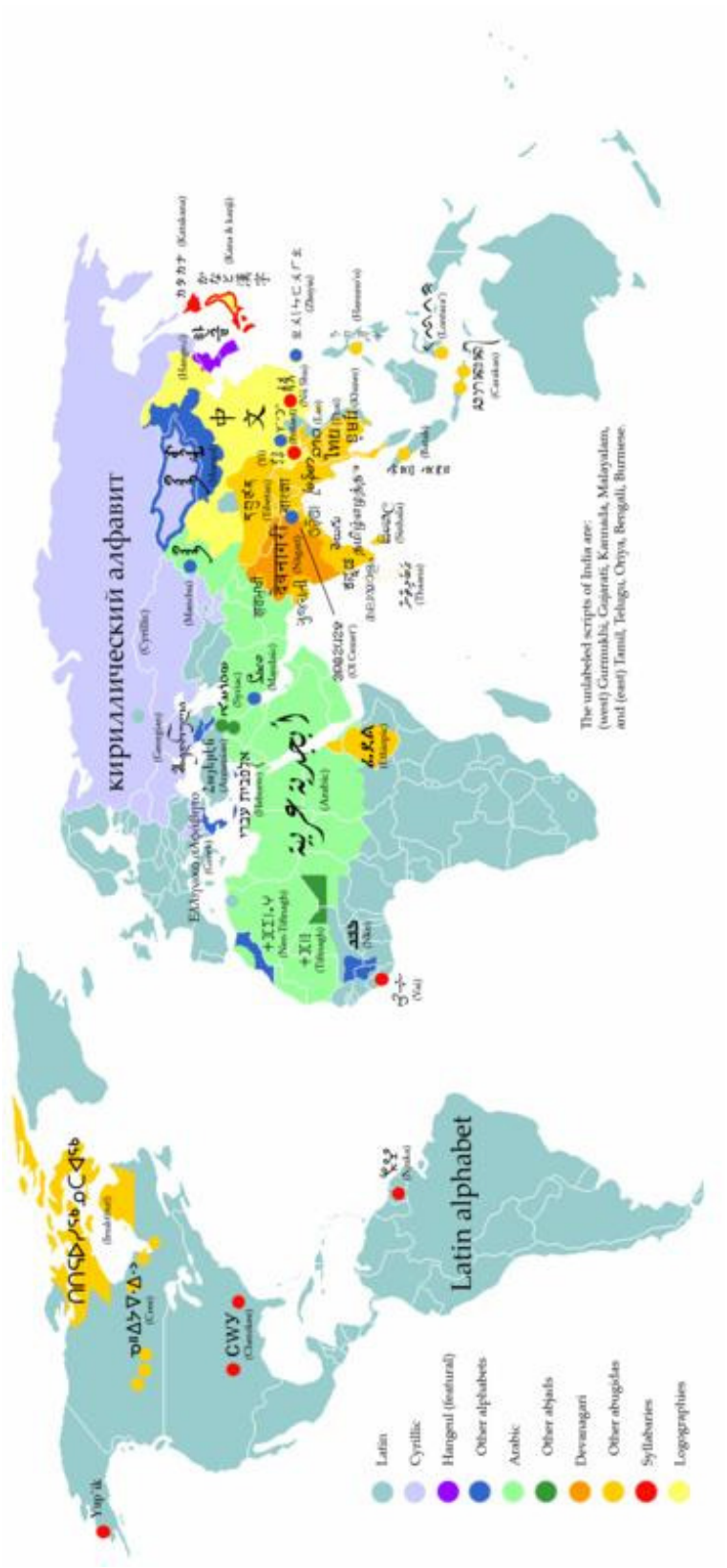


Figure A.1 Writing systems of the world

Reference: Wikipedia Contributors. (2008b, August 27). *Writing system*, [Online]. Wikipedia the Free Encyclopedia.

Available: http://en.wikipedia.org/wiki/Image:WritingSystemsoftheWorld4.png [2008, September 1].

Legend of writing systems of the world today:

- Latin (alphabetic)
- Cyrillic (alphabetic)
- Hangul (featural alphabetic)
- Other alphabets
- Arabic (abjad)
- Other abjads
- Devanagari (abugida)
- Other abugidas
- Syllabaries
- Chinese characters (logographic)

Table A.1 Functional classification of writing systems

Type	Symbol Representation	Example
Pictographic	Pictorgram or iconic picture	Hieroglyph, Cuneiform
Ideographic	Ideogram	Way-finding sign, mathematical notation
Logographic	Morpheme	Chinese character
Syllabic	Syllable	Japanese kana
Alphabetic	Phoneme (consonant or vowel)	Latin alphabet
Abugida	Phoneme (consonant + vowel)	Indian Devanāgarī
Abjad	Phoneme (consonant)	Arabic alphabet
Featural	Phonetic feature	Korean hangul

Table A.2 List of languages by number of native speakers

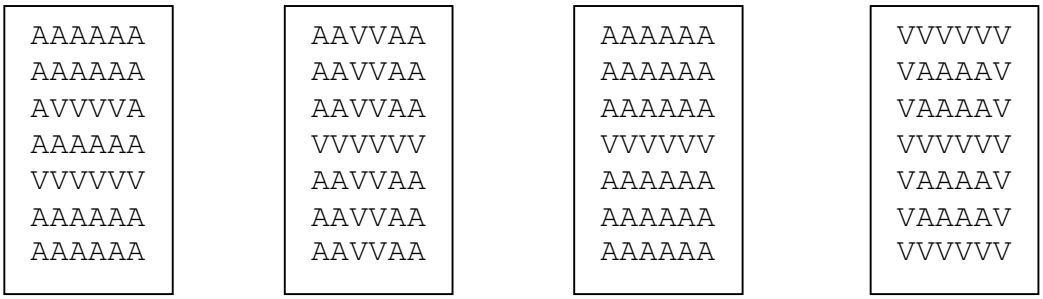
Language	Family	Ethnologue (Y2005)
1. Mandarin	Sino-Tibetan, Chinese	873,000,000
2. Hindi + Urdu	Indo-European, Indo-Iranian, Indo-Aryan	366,000,000
3. Spanish	Indo-European, Italic, Romance	358,000,000
4. English	Indo-European, Germanic, West	341,000,000
5. Arabic	Afro-Asiatic, Semitic	206,000,000
6. Portuguese	Indo-European, Italic, Romance	177,500,000
7. Bengali	Indo-European, Indo-Iranian, Indo-Aryan	171,000,000
8. Russian	Indo-European, Slavic, East	170,000,000
9. Japanese	Japanese-Ryukyuan	122,000,000
10. German	Indo-European, Germanic, West	100,000,000
11. Punjabi	Indo-European, Indo-Iranian, Indo-Aryan	88,000,000
12. French	Indo-European, Italic, Romance	79,572,000
13. Wu	Sino-Tibetan, Chinese	77,200,000
14. Javanese	Austronesian, Malayo-Polynesian, Sunda-Sulawesi	75,500,000
15. Korean	Considered either language isolate or Altaic	74,000,000
16. Telugu	Dravidian, South Central	69,700,000
17. Marathi	Indo-European, Indo-Iranian, Indo-Aryan	68,000,000
18. Vietnamese	Austro-Asiatic, Mon-Khmer, Vietic	67,400,000
19. Tamil	Dravidian, Southern	66,000,000
20. Italian	Indo-European, Italic, Romance	61,500,000
21. Cantonese	Sino-Tibetan, Chinese	54,800,000
22. Sindhi	Indo-European, Indo-Iranian, Indo-Aryan	54,500,000
23. Turkish	Altaic, Turkic, Oghuz	50,625,000
24. Min	Sino-Tibetan, Chinese	46,200,000
25. Gujarati	Indo-European, Indo-Iranian, Indo-Aryan	46,100,000
26. Maithili	Indo-European, Indo-Iranian, Indo-Aryan	45,000,000
27. Polish	Indo-European, Slavic, West	42,700,000
28. Ukrainian	Indo-European, Slavic, East	39,400,000
29. Persian	Indo-European, Indo-Iranian, Iranian	39,400,000
30. Malayalam	Dravidian, Southern - India	35,800,000
31. Kannada	Dravidian, Southern	35,400,000
32. Tamazight	Afro-Asiatic, Berber, Northern	32,300,000

Ref.: Wikipedia Contributors. (2008a, July 22). List of languages by number of native speakers, [Online]. Wikipedia the Free Encyclopedia. Available: http://en.wikipedia.org/w/index.php?title=List_of_languages_by_number_of_native_speakers&oldid=227300820 [2008, July 23].

APPENDIX B CHILD-MADE 2D KEYS

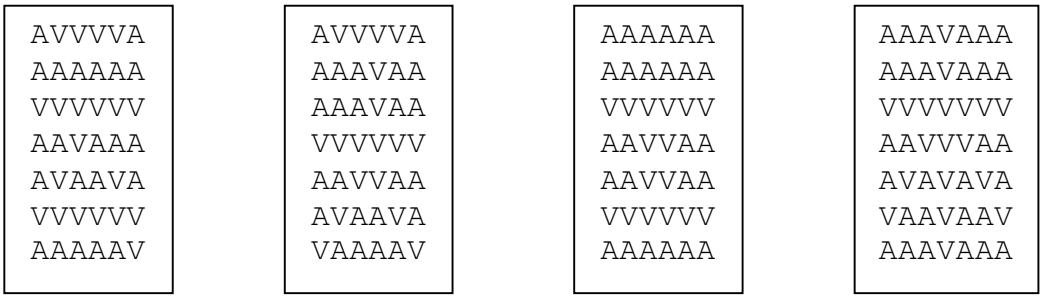
Authored by Wei-Tong Chui (徐伟栋), Wei-Jian Chui (徐伟坚), and Kok-Wah Lee (李国华)
in January 2009

In this part, it is shown that children are also capable to create simple 2D keys by using the key styles of ASCII art to draw some Chinese characters. The authors of these child-made 2D keys in January 2009 in this Appendix B were 13-year-old Wei-Jian Chui born in year 1996 (Figure B.1) and 9-year-old Wei-Tong Chui born in year 2000 (Figure B.2). To get the key size of every 2D key, just multiply the number of ASCII characters of a 2D key by the value of 6.57 bits, or to be more accurate $\log_2 95$. A note here: Kok-Wah Lee being the main author has integrated each four Chinese characters created by them to form a meaningful Chinese phrase for easy remembrance.



Two [二] Ten [十] One [一] Day [日]

Figure B.1 2D keys using ASCII art and Chinese characters meaning “twenty one days” [二十一日]



Cloud [云] Sky [天] Job [工] Wood [木]

Figure B.2 2D keys using ASCII art and Chinese characters meaning “cloudy sky nurtures the woods” [云天工木]

APPENDIX C CHRONOLOGY OF MY PhD STUDY

Table C.1 shows the important events during Kok-Wah Lee's PhD study at FET (Faculty of Engineering & Technology) of MMU (Multimedia University) in Bukit Beruang, Melaka, Malaysia from November 2003 to April 2011.

Table C.1 Development timeline of K. W. Lee's research project

Date	Event of Development Timeline
12 Nov. 2003	Application form of research project submitted to MMU CRPP.
27 May 2004	Official registration of doctorate (aka PhD) project.
14 Mar. 2005	Proposal defence seminar. Pass result.
19 Sep. 2005	Solid idea completion date for anti-hacking data storage using improved DIP switch.
14 Oct. 2005	Solid idea completion date for 2D (two-dimensional) key input method.
Oct. 2005	Kok-Wah Lee the student claimed for thesis submission, but Hong-Tat Ewe the nominal supervisor claimed for prototypes, and at least one accepted journal plus one submitted journal, or a journal replaced by an international patent (?).
24 May 2006	Solid idea completion date for MePKC (Memorizable Public Key Cryptography).
05 Nov. 2006	Software prototype of 2D key input method (version 1.1) was completed.
24 Nov. 2006	Software prototype of MobileECC (version 1.2) to test the MePKC encryption scheme and signature scheme was completed.
24 Nov. 2006	Kok-Wah Lee claimed for completion of prototypes.
29 Nov. 2006	Hardware prototype of RJ45 switch was completed.
14 Dec. 2006	Solid idea completion date for multihash key.
Jan. 2007	Software prototype to test the feasibility of multihash key was completed.
May 2007	Kok-Wah Lee claimed for fulfillment of minimum conditions to have at least one accepted journal and one submitted journal.
18 Feb. 2008	First work completion seminar.
01 April 2008	Result of first work completion seminar: Fail. More novel works were requested.
02 Jul. 2008	Second work completion seminar.
23 Jul. 2008	Result of second work completion seminar: Pass. The student entered ABD (All but Dissertation) stage.
23 Jul. 2008	Kok-Wah Lee submitted notice of thesis submission to FET and IPS.
21 Sep. 2008	Integration of multihash key into 2D key to produce 2D key input method (version 2.0).
25 Oct. 2008	Stop of literature study. First draft of PhD thesis (version 1.0) was ready.
01 Dec. 2008	Approval of specific thesis title.
14 Mar. 2009	Electronic online archive-type publication at www.archive.org.
25 Mar. 2009	Approval and confirmation of external expert examiners' list.

01 Apr. 2009	First submission of thesis draft (version 1.0) to IPS was rejected due to format.
06 Apr. 2009	First submission of thesis draft (version 1.0) to IPS again was accepted.
14 Apr. 2009	IPS letter stating completion of PhD study.
18 Aug. 2009	Electronic plagiarism detection using software was requested by IPS, but Kok-Wah Lee asked for postponement by not giving the electronic copy of thesis.
25 Aug. 2009	First open viva (aka oral exam). K.W. Lee was absent due to collisions of intellectual property rights with new MMU Rules and Regulations governing the thesis examination process. Moreover, short of preparation time from notice to oral exam. Fail result.
28 Oct. 2009	IPS rejected the PhD thesis and considered examination fail.
09 Nov. 2009	K.W. Lee's written letter requesting IPS for clarification on appropriate progress of PhD candidature.
13 Jan. 2010	IPS oral reply via A.W.C. Tan on termination of PhD candidature.
18 Jan. 2010	Written appeal for reinstatement of PhD candidature.
08 Feb. 2010	PhD candidature conditionally reinstated. The conditions were K.W. Lee to fulfill the MMU University Rules and Regulations, as well as medical certification on K.W. Lee's fitness to sit for the PhD thesis examination.
04 Mar. 2010	K.W. Lee's written letter to IPS for second thesis submission.
17 Mar. 2010	Second draft of PhD thesis (version 2.0) was ready.
18 Mar. 2010	IPS requested for oral exam directly without second round of thesis submission and K.W. Lee's signed declaration to fulfill any possible MMU University Rules and Regulations governing the thesis examination process.
30 Mar. 2010	K.W. Lee secondly applied for and reasoned on the second round of thesis submission to fulfill the IPS conditions.
20 Aug. 2010	Second open viva (aka oral exam) chaired by three thesis reviewers, a chairman, who was Kek-Kiong Tio (Mr.) (Dr.) having expertise in mechanical engineering, and another five committee members. Kok-Wah Lee attended the event. Fail result. PhD thesis was rejected and required major revisions of format and contents.
22 Sep. 2010	Reviewers' comments over the PhD thesis were received by Kok-Wah Lee from IPS. A maximum of one year was given before the re-submission of PhD thesis for re-examination.
22 Dec. 2010	The requested works to count the real entropy of Chinese password in ASCII encoding by the thesis examiners were dropped by removing the contents of Chinese password in the thesis. Alan Wee-Chiat Tan the nominal supervisor requested for revised abstract to locate a new batch of external thesis examiners.
24 Dec. 2010	Kok-Wah Lee submitted the updated abstract to A. W. C. Tan but rejected due to format. A series of disputes on MMU thesis format occurred later for weeks.
14 Jan. 2011	K. W. Lee asked the IPS for official and certified research thesis format acceptable by MMU, preferably at least one thesis sample was needed.
21 Mar. 2011	To fulfill the demand for acceptable thesis format by MMU, PhD supervisor was applied to be changed to V. C. Prasad (Vishnuvajjula Charan Prasad), who was a full professor at MMU FET.
30 Apr. 2011	Third draft of PhD thesis (version 3.0) was ready.

	Checking of copyright plagiarism over the thesis.
	Second submission of thesis draft (version 3.0) to IPS again was accepted (?). Thesis examination fee at MYR$600 was paid by K. W. Lee.
	Third open viva (aka oral exam).
	MMU senate letter on award of normal doctorate degree (i.e. Ph.D.).
	Convocation day.

N.B. 1: MMU = Multimedia University, which is a brand name of UTSB.

N.B. 2: UTSB = Universiti Telekom Sdn. Bhd., Malaysia.

N.B. 3: Sdn. Bhd. (Sendirian Berhad) in Malayan language, i.e. private limited in English language.

N.B. 4: FET = Faculty of Engineering & Technology, MMU, Bukit Beruang, Melaka, Malaysia.

N.B. 5: CRPP = Center for Research and Postgraduate Programmes, now called IPS, MMU.

N.B. 6: IPS = Institute for Postgraduate Studies, previously called CRPP, MMU.

REFERENCES

[1] Abadi, M., Bharat, K., and Marais, J. (2000, October 31). *System and method for generating unique passwords*. USPTO Issued Patent US6141760, Filing Date: 31 October 1997, Issue Date: 31 October 2000.

[2] Abadi, M., Lomas, T. M. A., and Needham, R. (1997, December 16). *Strengthening passwords* (Tech. Rep. No. SRC-1997-033). Palo Alto, CA, USA: Hewlett-Packard Company, HP Labs, Systems Research Center (SRC).

[3] Abadi, M., Needham, R. M., and Lomas, T. M. A. (2000, June 20). *Method and apparatus for strengthening passwords for protection of computer systems*. USPTO Issued Patent US6079021, Filing Date: 2 June 1997, Issue Date: 20 June 2000.

[4] Adams, A., and Sasse, M. A. (1999, December). Users are not the enemy. *Communications of the ACM, 42*(12), 41-46.

[5] Adams, A., Sasse, M. A., and Lunt, P. (1997, August 12-15). Making Passwords Secure and Usable. *Proceedings of the HCI on People and Computers XII*, Bristol, UK, 1-19.

[6] Allan, A. (2004, December 6). *Passwords are near the breaking point* (Tech. Rep. No. Gartner G00124970). Stamford, CT, USA: Gartner, Inc.

[7] Anderson, R. (2001). *Security engineering: A guide to building dependable distributed systems*. New York, NY, USA: John Wiley & Sons, Inc.

[8] Anderson, R. J., and Petitcolas, F. A. P. (1998, May). On the limits of steganography. *IEEE Journal on Selected Areas in Communications, 16*(4), 474-481.

[9] Arnold, M., Schmucker, M., and Wolthusen, S. D. (2003). *Techinques and applications digital watermarking and content protection*. Norwood, MA, USA: Artech House, Inc.

[10] Baddeley, A. D., Thomson, N., and Buchanan, M. (1975, December). Word length and the structure of short-term memory. *Journal of Verbal Learning and Verbal Behavior, 14*(6), 575-589.

[11] Bailey, J. R. (1969, December 23). *Slide switch*. USPTO Issued Patent US3485966, Filing Date: 2 October 1968, Issue Date: 2 October 1968.

[12] Baltzley, C. A. (2000, November 28). *Public key cryptosystem with roaming user capability*. USPTO Issued Patent US6154543, Filing Date: 25 November 1998, Issue Date: 28 November 2000.

[13] Baltzley, C. A. (2001a, August 16). *Public key cryptosystem with roaming user capability*. USPTO Published Patent Application US2001/0014158, Filing Date: 28 March 2001.

[14] Baltzley, C. A. (2001b, September 18). *Public key cryptosystem with roaming user capability*. USPTO Issued Patent US6292895, Filing Date: 19 June 2000, Issue Date: 18 September 2001.

[15] Barker, E., Barker, W., Burr, W., Polk, W., and Smid, M. (2007a, March). *Recommendation for key management – Part 1: General (revised)* (NIST Special Publication 800-57). Gaithersburg, MD, USA: CSRC (Computer Security Resource Center), NIST, 61-71.

[16] Barker, E., Barker, W., Burr, W., Polk, W., and Smid, M. (2007b, March). *Recommendation for key management – Part 2: Best practices for key management organization* (NIST Special Publication 800-57). Gaithersburg, MD, USA: CSRC (Computer Security Resource Center), NIST.

[17] Barker, E., and Kelsey, J. (2007, March). *Recommendation for random number generation using deterministic random bit generators (revised)* (NIST Special Publication 800-90). Gaithersburg, MD, USA: CSRC (Computer Security Resource Center), NIST.

[18] Barni, M., and Bartolini, F. (2004). *Watermarking systems engineering: Enabling digital assets security and other applications*. New York, NY, USA: Marcel Dekker, Inc.

[19] Beach, G. [2001, April 15]. *How do we manage our expanding collections of passwords and PINs?*, [Online]. CIO.com. Available: http://www.cio.com/article/print/30161 [2008, September 10].

[20] Beaver, K. (2004). *Hacking for dummies*. Indianapolis, Indiana, USA: Wiley Publishing, Inc.

[21] Bishop, M. (2003). *Computer security: Art and science*. Boston, MA, USA: Addison-Wesley.

[22] Blake, I., Seroussi, G., and Smart, N. (1999, July). *Elliptic curves in cryptography*. In London Mathematical Society Lecture Note Series (No. 265). Cambridge, Cambridgeshire, UK: Cambridge University Press.

[23] Blake, I. F., Seroussi, G., and Smart, N. P. (Eds.). (2005, April). *Advances in elliptic curve cryptography*. In London Mathematical Society Lecture Note Series (No. 317). Cambridge, UK: Cambridge University Press.

[24] Blaze, M., Diffie, W., Rivest, R. L., Schneier, B., Shimomura, T., Thompson, E., and Wiener, M. (1996). *Minimal key lengths for symmetric ciphers to provide adequate commercial security*. Chicago, Illinois, USA: A Report by an Ad Hoc Group of Cryptographers and Computer Scientists.

[25] Blonder, G. (1996, September 24). *Graphical password*. USPTO Issued Patent US5559961, Filing Date: 30 August 1995, Issue Date: 24 September 1996.

[26] Boatwright, M., and Luo, X. (2007, September 28-29). What do we know about biometrics authentication? *ACM Proceedings of the 4th Annual Conference on Information Security Curriculum Development 2007*, Kennesaw, Georgia, USA, 205-209.

[27] Boneh, D., and Franklin, M. (2006, September 26). *Systems and methods for identity-based encryption and related cryptographic techniques*. USPTO Issued Patent US7113594, Filing Date: 13 August 2002, Issue Date: 26 September 2006.

[28] Borenstein, N., and Freed, N. (1992, June). Base64 content-transfer-encoding. In *Request for comments (1341): MIME (Multipurpose Internet Mail Extensions): Mechanisms for specifying and describing the format of Internet message bodies* (RFC 1341). Sterling, Virginia, USA: Network Working Group, The Internet Engineering Task Force (IETF).

[29] Brainard, J., Juels, A., Rivest, R. L., Szydlo, M., and Yung, M. (2006, October 30 – November 3). Fourth-factor authentication: Somebody you know. *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 2006)*, Alexandria, Virginia, USA, 168-178.

[30] Brown, A. S., Bracken, E., Zoccoli, S., and Douglas, K. (2004, June 15). Generating and remembering passwords. *Applied Cognitive Psychology, 18*(6), 641-651.

[31] Brown, R. P. (1983, June 21). *Side actuated miniature DIP switch*. USPTO Issued Patent US4389549, Filing Date: 23 November 1981, Issue Date: 21 June 1983.

[32] Burgess, C., and Power, R. (2008, February 8). *Secrets stolen, fortunes lost: Preventing intellectual property theft and economic espionage in the 21st century*. Burlington, MA, USA:

Syngress Publishing (now is at Elsevier's Science & Technology publishing) (URL: http://www.syngress.com) (URL: http://www.elsevierdirect.com).

[33] Cachin, C. (1998, April 14-17). An information-theoretic model for steganography. *Proceedings of the 2nd International Workshop on Information Hiding (IH '98)*, LNCS 1525, Portland, Oregon, USA, 306-318.

[34] Cameron, K. (2005, May). *The laws of identity*, [Online]. Microsoft Corporation. Available: http://msdn.microsoft.com/en-us/library/ms996456.aspx [2008, August 25].

[35] Cameron, K., and Jones, M. B. (2006, January). *Design rationale behind the identity metasystem architecture*, [Online]. Microsoft Corporation. Available: http://research.microsoft.com/~mbj/papers/Identity_Metasystem_Design_Rationale.pdf [2008, August 25].

[36] Campbell, J., and Easter, R. J. (2007b, October 18). *Security requirements for cryptographic modules (Annex C): Approved random number generators for FIPS PUB 140-2* (draft) (NIST FIPS Pub 140-2 Annex C (Draft)). Gaithersburg, MD, USA: CSRC (Computer Security Resource Center), NIST.

[37] Cavoukian, A. (2006, October). *7 laws of identity: The case for privacy-embedded laws of identity in the digital age*, [Online]. IPC (Office of the Information and Privacy Commissioner) in Ontario, Canada. Available: http://www.ipc.on.ca/images/Resources/up-7laws_whitepaper.pdf [2008, August 25].

[38] Cayre, F., Fontaine, C., and Furon, T. (2005a, January 17-20). Watermarking security part one: Theory. *Proceedings of the SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents VII*, Vol. 5681, San Jose, CA, USA, 746-757.

[39] Cayre, F., Fontaine, C., and Furon, T. (2005b, January 17-20). Watermarking security part two: Practice. *Proceedings of the SPIE Conference on Security, Steganography, and Watermarking of Multimedia Contents VII*, Vol. 5681, San Jose, CA, USA, 758-768.

[40] Cayre, F., Fontaine, C., and Furon, T. (2005c, October). Watermarking security: Theory and practice. *IEEE Transcations on Signal Processing, 53*(10), 3976-3987.

[41] Cohen, H., and Frey, G. (2006). *Handbook of elliptic and hyperelliptic curve cryptography*. Boca Raton, FL, USA: Taylor & Francis Group, Chapman & Hall/CRC.

[42] Collberg, C. S., and Thomborson, C. (2002, August). Watermarking, tamper-proofing, and obfuscation – Tools for software protection. *IEEE Transactions on Software Engineering, 28*(8), 735-746.

[43] Cowan, N. (2001). The magical number 4 in short-term memory: A reconsideration of mental storage capacity. *Behavioral and Brain Sciences* [Online], *24*(1), 87–185. Available: http://www.bbsonline.org/documents/a/00/00/04/46/index.html [2008, July 21].

[44] Cox, I. J., Doërr, G., and Furon, T. (2006, November 8-10). Watermarking is not cryptography. *Proceedings of the 5th International Workshop on Digital Watermarking 2006 (IWDW 2006)*, LNCS 4283, Jeju Island (aka Jejudo), Jeju Province (aka Jeju-do), South Korea, 1-15.

[45] *Cryptographic Key Length Recommendation*, [Online]. (No date). Available: http://www.keylength.com [2008, October 23].

[46] Davies, J. H. E. (1997, March 4). *Personal identification devices and access control systems*. USPTO Issued Patent US5608387, Filing Date: 26 May 1994, Issue Date: 4 March 1997.

[47] de Koning Gans, G., Hoepman, J.-H., and Garcia F. D. (2008, September 8-11). A practical attack on the MIFARE Classic. *Proceedings of the 8th IFIP WG 8.8/11.2 International Conference on Smart Card Research and Advanced Applications (CARDIS 2008)*, London, England, UK, 267-282.

[48] de Winter, B. (2008, October 7). Researchers show how to crack popular smart cards. *InfoWorld*, [Online]. Available: http://www.infoworld.com/article/08/10/07/Researchers_show_how_to_crack_popular_smart_cards_1.html [2008, October 16].

[49] Dharmarajan, M. R. (2005, June 16). *Method and apparatus for password generation*. USPTO Published Patent Application US2005/0132203, Filing Date: 12 December 2003.

[50] Diffie, W., and Hellman, M. E. (1976, November). New directions in cryptography. *IEEE Transaction on Information Theory, IT-22*(6), 644-654.

[51] Diffie, W., and Woods, W. A. (2006, June 22). *Method for generating mnemonic random passcodes*. USPTO Published Patent Application US2007/0300076, Filing Date: 22 June 2006.

[52] Domenicone, R. (2000, May 3). *Safety box assembly*. EPO Published Patent Application EP0703341, Filing Date: 25 September 1995.

[53] Doumont, J.-L. (2002, June). Magical numbers: the seven-plus-or-minus-two myth. *IEEE Transactions on Professional Communication, 45*(2), 123-127.

[54] Eastlake, D. 3rd, Crocker, S., and Schiller, J. (1994, December). *Request for comments (1750): Randomness recommendations for security* (RFC 1750). Sterling, Virginia, USA: Network Working Group, The Internet Engineering Task Force (IETF).

[55] Eggers, J. J., Su, J. K., and Girod, B. (2000). *Asymmetric watermarking schemes*, [Online]. Available: http://citeseer.ist.psu.edu/eggers00asymmetric.html [2008, July 17].

[56] Ellis, N. C., and Hennelly, R. A. (1980). A bilingual word-length effect: Implications for intelligence testing and the relative ease of mental calculation in Welsh and English. *British Journal of Psychology, 71*, 43-51.

[57] Engelfriet, A. (2010, January/February). Choosing an open source license. *IEEE Software, 27*(1), 48-49.

[58] Farnell. (2007). *The Farnell inOne catalogue 2007/2008*, [Book, Online]. Available: http://my.farnell.com [2008, January 24].

[59] Florencio, D., and Herley, C. (2007, May 8-12). A large-scale study of web password habits. *Proceedings of the 16th ACM International Conference on World Wide Web*, Banff, Alberta, Canada, 657-666.

[60] Fonseca, D. E. (2003, December 9). *Data line switch*. USPTO Issued Patent US6660950, Filing Date: 24 July 2001, Issue Date: 9 December 2003.

[61] Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A., and Stewart, L. (1999, June). *Request for comments (2617): HTTP authentication: Basic and digest access authentication* (RFC 2617). Sterling, Virginia, USA: Network Working Group, The Internet Engineering Task Force (IETF).

[62] Fridrich, J., and Goljan, M. (2004, December 14). *Reliable detection of LSB steganography in color and grayscale images*. USPTO Issued Patent US6831991, Filing Date: 22 June 2001, Issued Date: 14 December 2004.

[63] Fridrich, J., Goljan, M., and Soukal, D. (2004, January 18-22). Searching for the stego-key. *Proceedings of the SPIE on Security, Steganography, and Watermarking of Multimedia Contents VI*, San Jose, California, USA, 70-82.

[64] Fried, I., and Evers, J. (2006, February 14). *Gates: End to passwords in sight*, [Online]. CNET Networks, Inc. Available: http://news.cnet.com/Gates-End-to-passwords-in-sight/2100-7355_3-6039177.html?tag=nw.11 [2008, August 23].

[65] Fumy, W., and Landrock, P. (1993, June). Principles of key management. *IEEE Journal on Selected Areas in Communications, 11*(5), 785-793.

[66] Furht, B., and Kirovski, D. (2006a, April 18). *Multimedia watermarking techniques and applications*. Boca Raton, FL, USA: Taylor & Francis Group, Auerbach Publications.

[67] Furht, B., and Kirovski, D. (2006b, May 3). *Multimedia encryption and authentication techniques and applications*. Boca Raton, FL, USA: Taylor & Francis Group, Auerbach Publications.

[68] Furnell, S. (2005, March). Authenticating ourselves: will we ever escape the password? *Network Security, 2005*(3), 8-13.

[69] Furon, T. (2005, September 15-17). A survey of watermarking security. *Proceedings of the 4th International Workshop on Digital Watermarking 2005 (IWDW 2005)*, LNCS 3710, Siena, Tuscany, Italy, 201-215.

[70] Furon, T., and Duhamel, P. (2003, April). An asymmetric watermarking method. *IEEE Transactions on Signal Processing, 51*(4), 981-995.

[71] Gabber, E., Gibbons, P. B., Matias, Y., and Mayer, A. (1997, February 24-28). How to make personalized web browsing simple, secure, and anonymous. *Proceedings of 1st International Conference on Financial Cryptography 1997 (FC 1997)*, LNCS 1318, Anguilla, British West Indies, 17-31.

[72] Ganesan, R. (1996a, July 9). *Yaksha, an improved system and method for securing communications using split private key asymmetric cryptography*. USPTO Issued Patent US5535276, Filing Date: 9 November 1994, Issue Date: 9 July 1996.

[73] Ganesan, R. (1996b, September 17). *System and method for centralized session key distribution, privacy enhanced messaging and information distribution using a split private*

key public cryptosystem. USPTO Issued Patent US5557678, Filing Date: 18 July 1994, Issue Date: 17 September 1996.

[74] Ganesan, R. (1998a, April 7). *Computer system for securing communications using split private key asymmetric cryptography*. USPTO Issued Patent US5737419, Filing Date: 7 June 1996, Issue Date: 7 April 1998).

[75] Ganesan, R. (1998b, May 5). *Securing E-mail communications and encrypted file storage using yaksha split private key asymmetric cryptography*. USPTO Issued Patent US5748735, Filing Date: 7 June 1996, Issue Date: 5 May 1998.

[76] Ganesan, R. (1998c, November 17). *Computer system for centralized session key distribution, privacy enhanced messaging and information distribution using a split private key public cryptosystem*. USPTO Issued Patent US5838792, Filing Date: 8 August 1996, Issue Date: 17 November 1998.

[77] Ganesan, R. (1999, May 18). *Programmed computer for identity verification, forming joint signatures and session key agreement in an RSA public cryptosystem*. USPTO Issued Patent US5905799, Filing Date: 15 October 1996, Issue Date: 18 May 1999.

[78] Ganesan, R., Sandhu, R. S., Cottrell, A. P., and Austin, K. (2006a, May 31). *Augmented single factor split key asymmetric cryptography-key generation and distributor*. USPTO Published Patent Application US2007/0033392, Filing Date: 31 May 2006.

[79] Ganesan, R., Sandhu, R. S., Cottrell, A. P., and Austin, K. (2006b, May 31). *Secure login using augmented single factor split key asymmetric cryptography*. USPTO Published Patent Application US2007/0186095, Filing Date: 31 May 2006.

[80] Ganesan, R., Sandhu, R. S., Cottrell, A. P., and Austin, K. (2006c, May 31). *Secure login using single factor split key asymmetric cryptography and an augmenting factor*. USPTO Published Patent Application US2007/0033393, Filing Date: 31 May 2006.

[81] Ganesan, R., Sandhu, R. S., Cottrell, A. P., Schoppert, B. J., and Bellare, M. (2006, May 2). *Protecting one-time-passwords against man-in-the-middle attacks*. USPTO Published Patent Application, US2007/0033642, Filing Date: 2 May 2006.

[82] Ganesan, R., and Yacobi, Y. (1996, December 24). *System and method for identity verification, forming joint signatures and session key agreement in an RSA public*

cryptosystem. USPTO Issued Patent US5588061, Filing Date: 20 July 1994, Issue Date: 24 December 1996.

[83] Garcia, F. D., de Koning Gans, G., Muijrers, R., van Rossum, P., Verdult, R., Schreur, R. W., and Jacobs, B. (2008, October 6-8). Dismantling MIFARE Classic. *Proceedings of the 13th European Symposium on Research in Computer Security (ESORICS 2008)*, Málaga, Andalusia, Spain, 97-114.

[84] Gehringer, E. F. (2002, June 6-8). Choosing passwords: Security and human factors. *Proceedings of the IEEE International Symposium on Technology and Society (ISTAS 2002)*, Raleigh, North Carolina, USA, 369-373.

[85] Gehrmann, C., and Näslund, M. (Eds.). (2005, March 1). *ECRYPT Yearly report on algorithms and keysizes (2004)* (Report No. IST-2002-507932 D.SPA.10). Katholieke Universiteit Leuven, Leuven-Heverlee, Belgium: European Network of Excellence in Cryptology (ECRYPT).

[86] Gehrmann, C., and Näslund, M. (Eds.). (2006, January 29). *ECRYPT Yearly report on algorithms and keysizes (2005)* (Report No. IST-2002-507932 D.SPA.21). Katholieke Universiteit Leuven, Leuven-Heverlee, Belgium: European Network of Excellence in Cryptology (ECRYPT).

[87] Gehrmann, C., and Näslund, M. (Eds.). (2007, January 26). *ECRYPT Yearly report on algorithms and keysizes (2006)* (Report No. IST-2002-507932 D.SPA.16). Katholieke Universiteit Leuven, Leuven-Heverlee, Belgium: European Network of Excellence in Cryptology (ECRYPT).

[88] Goal, P. M., and Kriese, S. J. (2004, August 26). *Method and system for automated password generation*. USPTO Published Patent Application US2004/0168068, Filing Date: 20 February 2003.

[89] Goldwasser, S. (1997, October 20-22). New directions in cryptography: twenty some years later (or cryptograpy and complexity theory: a match made in heaven). *Proceedings of the 38th Annual Symposium on Foundations of Computer Science (SFCS 1997)*, Miami Beach, Fl, USA, 314-324.

[90] Gouda, M. G., Liu, A. X., Leung, L. M., and Alam, M. A. (2005, June 7-10). Single password, multiple accounts. *Proceedings of the 3rd International Conference on Applied*

Cryptography and Network Security (ACNS 2005), LNCS 3531, New York City, NY, USA, Industry / Short Paper Track, 1-12.

[91] Hachez, G., and Quisquater, J.-J. (2002). *Which directions for asymmetric watermarking?*, [Online]. Available: http://citeseer.ist.psu.edu/564734.html [2008, July 17].

[92] Halderman, J. A., Waters, B., and Felten, E. W. (2005, May 10-14). A convenient method for securely managing passwords. *Proceedings of the 14th International Conference on World Wide Web 2005*, Chiba, Japan, 471-479.

[93] Hankerson, D., Menezes, A., and Vanstone, S. (2004). *Guide to elliptic curve cryptography*. New York, NY, USA: Springer-Verlag New York, Inc.

[94] Hankerson, D., Menezes, A., and Vanstone, S. (2005, August). *Guide to elliptic curve cryptography* [椭圆曲线密码学导论] (张焕国, Trans. to Chinese language). Beijing [北京], China [中国]: Publishing House of Electronics Industry [电子工业出版社]. (Original published in 2004 in English language).

[95] Haperen, P. V. (1997, May 16). *Graphical password entry*. UK Published Patent Application GB2313460, Filing Date: 16 May 1997.

[96] Hardesty, E. C. (1975, January 14). *Electrical connecting devices for terminating cords and methods of assembling the devices to cords*. USPTO Issued Patent US3860316, Filing Date: 6 July 1973, Issue Date: 14 January 1975.

[97] Hart, G. W. (1994, September). To decode short cryptograms. *Communications of the ACM, 37*(9), 102-108.

[98] Hartung, F., and Kutter, M. (1999, July). Multimedia watermarking techniques. *Proceedings of the IEEE, 87*(7), 1079-1107.

[99] Haylock, S. E. (No date). *Fingerprints*, [Online]. Answers.com. Available: http://www.answers.com/topic/fingerprints-5 [2008, September 1].

[100] Hoffman, N. E. (1982, June 1). *DIP swtich*. USPTO Issued Patent US4332987, Filing Date: 15 December 1980, Issue Date: 1 June 1982.

[101] Hoosain, R., and Salili, F. (1988). Language differences, working memory, and mathematical ability. *Practical aspects of memory: Current research and issues, 2*, 512-517.

[102] Huang, T. D. (1985, February 19). *Method for encoding Chinese characters*. USPTO Issued Patent US4500872, Filing Date: 18 March 1982, Issue Date: 19 February 1985.

[103] Ives, B., Walsh, K. R., Schneider, H. (2004, April). The domino effect of password reuse. *Communications of the ACM, 47*(4), 75-78.

[104] Jablon, D. P. (2006, March 7). *Cryptographic methods for remote authentication*. USPTO Issued Patent US7010692, Filing Date: 9 June 2004, Issue Date: 7 March 2006.

[105] Jermyn, I., Mayer, A., Monrose, F., Reiter, M., and Rubin, A. (1999, August 23-26). The design and analysis of graphical passwords. *Proceedings of 8th USENIX Security Symposium*, Washington D.C., USA, 1-14.

[106] Jones, D. M. (2002, October). *The 7±2 urban legend*, [Online]. MISRA C Conference. Available: http://citeseer.ist.psu.edu/jones02urban.html; http://www.knosof.co.uk/cbook/misart.pdf [2008, July 20].

[107] Jones, M. B. (2005, May). *Microsoft's vision for an identity metasystem*, [Online]. Microsoft Corporation. Available: http://msdn.microsoft.com/en-us/library/ms996422.aspx [2008, August 25].

[108] Kanaley, R. (2001, February 4). *Login error trouble keeping track of all your sign-ons? Here's a place to keep your electronic keys, but you'd better remember the password*. San Jose Mercury News.

[109] Karp, A. H. (2003, May 6). *Site-specific passwords* (Tech. Rep. No. HPL-2002-39R1). Palo Alto, CA, USA: Hewlett-Packard Company, HP Laboratories Palo Alto, Intelligent Enterprise Technologies Laboratory.

[110] Karp, A. H., and Poe, D. T. (2002, August 2). *System-specific passwords*. USPTO Published Patent Application US2004/0025026, Filing Date: 2 August 2002.

[111] Keller, S. S. (2005, January 31). *NIST-recommended random number generator based on ANSI X9.31 Appendix A.2.4 using the 3-key triple DES and AES algorithms*, [Online]. Gaithersburg, MD, USA: CSRC (Computer Security Resource Center), NIST. Available: http://csrc.nist.gov/groups/STM/cavp/documents/rng/931rngext.pdf [2008, May 19].

[112] Kelsey, J., Schneier, B., Hall, C., and Wagner, D. (1997, September 17-19). Secure applications of low-entropy keys. *Proceedings of the International Workshop on Information Security (ISW '97)*, LNCS 1396, Tatsunokuchi, Ishikawa, Japan, 121-134.

[113] Klein, D. V. (1990, August 27). "Foiling the cracker": A survey of, and improvements to, password security (revised paper). *Proceedings of the USENIX 2nd Security Workshop Program*, Portland, Oregon, USA, 5-14.

[114] Kormann, D. P., and Rubin, A. D. (2000, June). Risks of the Passport single signon protocol. *Computer Networks, 33*(1-6), 51-58.

[115] Kotadia, M. (2004, February 25). *Gates predicts death of the password*, [Online]. CNET Networks, Inc. Available: http://news.cnet.com/Gates-predicts-death-of-the-password/2100-1029_3-5164733.html?tag=nw.4 [2008, August 23].

[116] Kučera, H., and Francis, W. N. (1967). *Computational analysis of present-day American English*. Providence, Rhode Island, USA: Brown University Press.

[117] Kurokawa, K. (1988, July). Quality and innovation [Japanese electronics industry]. *IEEE Circuits and Devices Magazine, 4*(4), 3-8.

[118] Kurokawa, K. (1990, May 13-18). Quality and innovation. *Proceedings of the 1990 IEEE International Conference on Robotics and Automation (ROBOT 1990)*, Cincinnati, OH, USA, Vol. 3, 2180-2184.

[119] Kurokawa, K. (1991, January). Quality and innovation. *IEEE Control Systems Magazine, 11*(1), 47-51.

[120] Kurokawa, K. (1997, April/May). Modeling human interactions. *IEEE Potentials, 16*(2), Part 2, 26-28.

[121] LAN/MAN Standards Committee. (2005, December 9). *Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications*, [Online]. New York, NY, USA: IEEE Computer Society. Available: Access http://standards.ieee.org/getieee802/802.3.html (to get) http://standards.ieee.org/getieee802/download/802.3-2005_section2.pdf [2008, January 24].

[122] Le Quere, P. (2004, March 30). *High speed random number generation*. USPTO Issued Patent US6714955, Filing Date: 13 August 2001, Issue Date: 30 March 2004.

[123] Lee, K. W. (2005, September 19). *An nPST dual in-line package switch (DIL/DIP switch) linking all the little actuators into a single actuator*, [Electronic Component, Layout-Design of Integrated Circuit]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[124] Lee, K. W. (2006a, November 5). *2-dimensional key input method version 1.1*, [CD-ROM, Computer Program]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[125] Lee, K. W. (2006b, November 29). *An Ethernet cable RJ45 switch for securing data communication and storage using conventional dual in-line package switch (DIL/DIP switch)*, [Electronic Component, Layout-Design of Integrated Circuit]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[126] Lee, K. W. (2007a, January). *Account amount estimator of multihash key using key strengthening based on time response*, [CD-ROM, Computer Program]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[127] Lee, K. W. (2007b, October 19). *An (nPST + reverse mPST) dual in-line package switch (DIL/DIP switch) with two bigger actuators linking two groups of switches activated oppositely*, [Electronic Component, Layout-Design of Integrated Circuit]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[128] Lee, K. W. (2007c, December 11). *An Ethernet cable RJ45 switch for securing data communication and storage using Grayhill 78H02T (double 4PST DIP switch)*, [Electronic Component, Layout-Design of Integrated Circuit]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[129] Lee, K. W. (2007d, December 11). *An Ethernet cable RJ45 switch for securing data communication and storage using Grayhill 78H01T (single 4PST DIP switch)*, [Electronic Component, Layout-Design of Integrated Circuit]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[130] Lee, K. W. (2007e, December 11). *An Ethernet cable RJ45 switch for securing data communication and storage using Grayhill 78F01T (single 2PST DIP switch)*, [Electronic Component, Layout-Design of Integrated Circuit]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[131] Lee, K. W. (2008a, May 8). *An improved dual in-line (DIL) switch for securing data communication and storage*. Malaysia Application of Utility Innovation (aka utility model or

small patent) UI 20070733, MyIPO, Filing Date: 11 May 2007, Grant Date: 30 June 2010, Patent No.: MY-141830-A.

[132] Lee, K. W. (2008b, May 8). *An improved dual in-line (DIL) switch for securing data communication and storage*. PCT Patent Application PCT/MY2008/000040, WIPO, Filing Date: 8 May 2008, Publication Date: 20 November 2008.

[133] Lee, K. W. [李國華]. (2008c, May 9). *應用於保護資料通訊及存儲安全之改良式雙行開關* [An improved dual in-line (DIL) switch for securing data communication and storage]. Taiwan (ROC) Patent Application TW097117364, TIPO, Filing Date: 9 May 2008. (in Chinese language).

[134] Lee, K. W. (2008d, June 2). *A telephone cable RJ11 switch for securing data communication and storage using Grayhill 78H01T (single 4PST DIP switch)*, [Electronic Component, Layout-Design of Integrated Circuit]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[135] Lee, K. W. (2008e, June 2). *A telephone cable RJ11 switch for securing data communication and storage using Grayhill 78F01T (single 2PST DIP switch)*, [Electronic Component, Layout-Design of Integrated Circuit]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[136] Lee, K. W. (2008f, June 2). *A USB switch for securing data communication and storage using Grayhill 78H01T (single 4PST DIP switch)*, [Electronic Component, Layout-Design of Integrated Circuit]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[137] Lee, K. W. (2008g, June 2). *A USB switch for securing data communication and storage using Grayhill 78F01T (single 2PST DIP switch)*, [Electronic Component, Layout-Design of Integrated Circuit]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[138] Lee, K. W. (2008h, July 25). *Methods and systems to create big memorizable secrets and their applications in information engineering*. Malaysia Patent Application PI 20082771, MyIPO, Filing Date: 25 July 2008.

[139] Lee, K. W. (2008i, September 21). *2-dimensional key input method with multihash key version 2.0*, [CD-ROM, Computer Program]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[140] Lee, K. W. (2008j, September 21). *Mobile ECC version 2.0*, [CD-ROM, Computer Program]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[141] Lee, K. W. (2008k, December 10). *Methods and systems to create big memorizable secrets and their applications in information engineering*. Singapore Patent Application SG 200809162-1, IPOS, Filing Date: 10 December 2008, Now Abandoned.

[142] Lee, K. W. (2008l, December 18). *Methods and systems to create big memorizable secrets and their applications in information engineering*. PCT Patent Application PCT/IB2008/055432, WIPO, Filing Date: 18 December 2008, Publication Date: 28 January 2010.

[143] Lee, K. W. (2009a, March 14). *Memorizable public-key cryptography (MePKC) & its applications*, 1st ed. (version 1.0), [Online]. Internet Archive. Available: http://www.archive.org/details/MemorizablePublic-keyCryptographymepkcItsApplications [2010, March 08].

[144] Lee, K. W. (2009b, April). High-Entropy 2-Dimensional Key Input Method for Symmetric and Asymmetric Key Cryptosystems. *International Journal of Computer and Electrical Engineering (IJCEE), 1*(1), 1-8.

[145] Lee, K. W. (2009c, November 07). *2-dimensional key input method with multihash key version 3.0*, [CD-ROM, Computer Program]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[146] Lee, K. W. (2010a, September 11). *2-dimensional key input method with multihash key version 4.0*, [CD-ROM, Computer Program]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[147] Lee, K. W. (2010b, September 15). *Methods and systems to create big memorizable secrets and their applications in information engineering*. Singapore Patent Application SG 200809162-1, IPOS, Filing Date: 15 September 2010.

[148] Lee, K. W. (2010c, November 08). *Methods and systems to create big memorizable secrets and their applications in information engineering*. United States Patent Application US 2011/0055585, USPTO, Filing Date (Completion): 08 November 2010.

[149] Lee, K. W., and Ewe, H. T. (2006, November 3-6). Coinware for multilingual passphrase generation and its application for Chinese language password. *Proceedings of the 2006*

International Conference on Computational Intelligence and Security (CIS 2006), Guangzhou, Guangdong, China, 1511-1514 (Part 2).

[150] Lee, K. W., and Ewe, H. T. (2007, August). Multiple hashes of single key with passcode for multiple accounts. *Journal of Zhejiang University Science A (JZUS-A), 8*(8), 1183-1190.

[151] Lee, K. W., and Tan, A. W. C. (2006, November 24). *MobileECC version 1.2*, [CD-ROM, Computer Program]. Available: Lee, K. W., Bukit Beruang, Melaka, Malaysia.

[152] Lee, K. W., Teh, C. E., and Tan, Y. L. (2006, May 30-31). *Decrypting English text using enhanced frequency analysis*. Seminar conducted at the meeting of the National Seminar on Science, Technology and Social Sciences (STSS 2006), Kuantan, Pahang, Malaysia.

[153] Liataud, J. P., and Maloney, M. L. (1983, March 8). *DIP switch*. USPTO Issued Patent US4376234, Filing Date: 5 May 1981, Issue Date: 8 March 1983.

[154] Lilly, G. M. (2004, December 7). *Device for and method of one-way cryptographic hashing*. USPTO Issued Patent US6829355, Filing Date: 5 March 2001, Issue Date: 7 December 2004.

[155] Lin, H. C. (1999, October 19). *Dual inline package switch*. USPTO Issued Patent US5967302, Filing Date: 6 March 1998, Issue Date: 19 October 1999.

[156] Lockard, J. L. (1977, March 15). *Miniature switch with substantial wiping action*. USPTO Issued Patent US4012608, Filing Date: 25 March 1975, Issue Date: 15 March 1977.

[157] Lockard, J. L. (1979, September 18). *Impedance programming DIP switch assembly*. USPTO Issued Patent US4168404, Filing Date: 3 May 1978, Issue Date: 18 September 1979.

[158] *Log This*, [Online]. (No date). Available: http://members.lycos.co.uk/wuul/logthis/readme.html [2008, March 25].

[159] Low, S. H., and Maxemchuk, N. F. (1998, May). Performance comparison of two text marking methods. *IEEE Journal on Selected Areas in Communications, 16*(4), 561-572.

[160] Lu, C.-S. (2005). *Multimedia security: Steganography and digital watermarking techniques for protection of intellectual property*. Hershey, PA, USA: Idea Group Publishing.

[161] Luo, H., and Henry, P. (2003, September 7-10). A common password method for protection of multiple accounts. *Proceedings of the 14th IEEE 2003 International Symposium on*

Personal, Indoor and Mobile Radio Communication (PIMRC 2003), Beijing, China, vol. 3, 2749-2754.

[162] Macuch, P. L. (2005, November 22). *Coaxial and DSL cable switch for controlling a computer connection to the Internet*. USPTO Issued Design Patent D511749, Filing Date: 17 November 2003, Issue Date: 22 November 2005.

[163] Maghiros, I., Punie, Y., Delaitre, S., Lignos, E., Rodríguez, C., Ulbrich, M., Cabrera, M., Clements, B., Beslay, L., and van Bavel, R. (2005). *Biometrics at the frontiers: Assessing the impact on society* (Report No. EUR 21585 EN). Seville, Sevilla, Spain: European Commission, Joint Research Centre (JRC), Institute for Prospective Technological Studies (IPTS).

[164] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S. (2003). *Handbook of fingerprint recognition*. New York, NY, USA: Springer-Verlag New York, Inc.

[165] Manber, U. (1996). A simple scheme to make passwords based on one-way functions much harder to crack. *Computers & Security, 15*(2), 171-176.

[166] Markoff, J. (2008, October 20). A robot network seeks to enlist your computer. *The New York Times*, [Online]. Available: http://www.nytimes.com/2008/10/21/technology/internet/21botnet.html [2008, October 23].

[167] Marshall, D. (2003). *.NET security programming*. Indianapolis, IN, USA: Wiley.

[168] Matias, Y., Mayer, A., and Silberschatz, A. (1997, December 8-11). Lightweight security primitives for e-commerce. *Proceedings of the USENIX Symposium on Internet Technologies and Systems 1997*, Monterey, California, USA, 95-102.

[169] McCulligh, M. R. (2003, November 4). *Password generation method and system*. USPTO Issued Patent US6643784, Filing Date: 14 December 1998, Issue Date: 4 November 2003.

[170] McNamara, J. (2003). *Secrets of computer espionage: Tactics and countermeasures*. Indianapolis, Indiana, USA: Wiley Publishing, Inc.

[171] Menezes, A. J., Oorschot, P. C. V., and Vanstone, S. A. (1996). *Handbook of applied cryptography*. Boca Raton, FL, USA: CRC Press.

[172] Miller, G. A. (1956). The magical number seven, plus or minus two: Some limits on our capacity for processing information. *The Psychological Review, 63*(2), 81-97.

[173] Mittelholzer, T. (1999, September 29 – October 1). An information-theoretic approach to steganography and watermarking. *Proceedings of the 3rd International Workshop on Information Hiding (IH '99)*, LNCS 1768, Dresden, Saxony, Germany, 1-16.

[174] Mohanty, S. P. (1999). *Digital watermarking: A tutorial review*, [Online, Tech. Rep.]. Bangalore, Bayaluseeme, Karnataka, India: Indian Institute of Science. Available: http://citeseer.ist.psu.edu/572262.html [2008, July 17].

[175] Mollin, R. A. (2007a). *Codes: The guide to secrecy from ancient to modern times*. Boca Raton, FL, USA: Chapman & Hall/CRC, Taylor & Francis Group.

[176] Mollin, R. A. (2007b). *An introduction to cryptography* (2nd ed.). Boca Raton, FL, USA: Taylor & Francis Group, Chapman & Hall/CRC.

[177] Moseley, B. E. (2006, February 2). *Method and system for generating passwords*. USPTO Published Patent Application US2006/0026439, Filing Date: 2 August 2004.

[178] Moulin, P., and O'Sullivan, J. A. (2003, March). Information-theoretic analysis of information hiding. *IEEE Transactions on Information Theory, 49*(3), 563-593.

[179] NIST. (1995a, April 17). *Secure hash standard* (NIST FIPS Pub 180-1). Gaithersburg, MD, USA: CSRC (Computer Security Resource Center), NIST.

[180] NIST. (2002b, August 1). *Secure hash standard* (NIST FIPS Pub 180-2 (+ Change Notice to include SHA-224)). Gaithersburg, MD, USA: CSRC (Computer Security Resource Center), NIST.

[181] NIST. (2006c, March 13). *Secure signature standard (DSS)* (draft) (NIST FIPS Pub 186-3 (Draft)). Gaithersburg, MD, USA: CSRC (Computer Security Resource Center), NIST.

[182] NIST. (2007b, June 12). *Secure hash standard (SHS)* (draft) (NIST FIPS Pub 180-3 (Draft)). Gaithersburg, MD, USA: CSRC (Computer Security Resource Center), NIST.

[183] Ogletree, T. W. (2000). *Practical firewalls*. Indianapolis, Indiana, USA: Macmillan Computer Publishing, Que Corporation.

[184] *PasswordResearch.com*, [Online]. (No date). Available: http://www.passwordresearch.com [2008, September 10].

[185] Pelzl, J., Wollinger, T., and Paar, C. (2004, April 5-7). High performance arithmetic for special hyperelliptic curve cryptosystems of genus two. *Proceedings of the International Conference on Information Technology: Coding and Computing 2004 (ITCC 2004)*, Las Vegas, Nevada, USA, Vol. 2, 513-517.

[186] Petitcolas, F. A. P., Anderson, R. J., and Kuhn, M. G. (1999, July). Information hiding - A survey. *Proceedings of the IEEE: Special Issue on Protection of Multimedia Content, 87*(7), 1062-1078.

[187] PGP Corporation. (2006). *PGP Desktop 9.0 for windows user's guide*. Palo Alto, California, USA: PGP Corporation, 229-232.

[188] Rivest, R. (1992, April). *Request for comments (1321): The MD5 Message-Digest Algorithm* (RFC 1321). Sterling, Virginia, USA: Network Working Group, The Internet Engineering Task Force (IETF).

[189] Rivest, R. L., Shamir, A., and Adleman, L. (1978, February). A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM, 21*(2), 120-126.

[190] Rivest, R. L., Shamir, A., and Adleman, L. M. (1983, September 20). *Cryptographic communications system and method*. USPTO Issued Patent US4405829, Filing Date: 14 December 1977, Issue Date: 20 September 1983.

[191] Roellgen, C. B. (No date). *Scalable polymorphic hash function*, [Online]. Available: http://www.pmc-ciphers.com [2008, July 16].

[192] Ross, B., Jackson, C., Miyake, N., Boneh, D., and Mitchell, J. C. (2005, July 31 - August 5). Stronger password authentication using browser extensions. *Proceedings of the 14th USENIX Security Symposium (SEC 2005)*, Baltimore, MD, USA, 17-32.

[193] Rubin, K., and Silverberg, A. (2003, August 17-21). Torus-based cryptography. *Proceedings of the 23rd Annual International Cryptology Conference 2003 (CRYPTO 2003)*, LNCS 2729, Santa Barbara, California, USA, 349-365.

[194] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J., and Vo, S. (2001, May 15). *A statistical test suite for*

random and pseudorandom number generators for cryptographic applications (NIST Special Publication 800-22). Gaithersburg, MD, USA: CSRC (Computer Security Resource Center), NIST.

[195] Sandhu, R., deSa, C., and Ganesan, K. (2003, June 19). *One time password entry to access multiple network sites*. USPTO Published Patent Application US2003/0115452, Filing Date: 19 December 2000.

[196] Sandhu, R., deSa, C., and Ganesan, K. (2005a, April 19). *System and method for password throttling*. USPTO Issued Patent US6883095, Filing Date: 19 December 2000, Issue Date: 19 April 2005.

[197] Sandhu, R., deSa, C., and Ganesan, K. (2005b, September 6). *High security cryptosystem*. USPTO Issued Patent US6940980, Filing Date: 19 December 2000, Issue Date: 6 September 2005.

[198] Sandhu, R., deSa, C., and Ganesan, K. (2005c, November 29). *System and method for crypto-key generation and use in cryptosystem*. USPTO Issued Patent US6970562, Filing Date: 19 December 2000, Issue Date: 29 November 2005.

[199] Sandhu, R., deSa, C., and Ganesan, K. (2006a, March 21). *Secure communications network with user control of authenticated personal information provided to network entities*. USPTO Issued Patent US7017041, Filing Date: 19 December 2000, Issue Date: 21 March 2006.

[200] Sandhu, R., deSa, C., and Ganesan, K. (2006b, May 30). *One time password entry to access multiple network sites*. USPTO Issued Patent US7055032, Filing Date: 21 May 2004, Issue Date: 30 May 2006.

[201] Sandhu, R., deSa, C., and Ganesan, K. (2006c, June 20). *System and method for generation and use of asymmetric crypto-keys each having a public portion and multiple private portions*. USPTO Issued Patent US7065642, Filing Date: 19 December 2000, Issue Date: 20 June 2006.

[202] Sandhu, R., deSa, C., and Ganesan, K. (2006d, June 27). *System and method for authentication in a crypto-system utilizing symmetric and asymmetric crypto-keys*. USPTO Issued Patent US7069435, Filing Date: 19 December 2000, Issue Date: 27 June 2006.

[203] Sandhu, R., deSa, C., and Ganesan, K. (2006e, November 2). *Laddered authentication security using split key asymmetric cryptography*. USPTO Published Patent Application US2006/0248333, Filing Date: 22 June 2006.

[204] Sandhu, R., deSa, C., and Ganesan, K. (2006f, December 12). *Method and system for authorizing generation of asymmetric crypto-keys*. USPTO Issued Patent US7149310, Filing Date: 19 December 2000, Issue Date: 12 December 2006.

[205] Sandhu, R. S., Ganesan, R., Cottrell, A. P., Renshaw, T. S., Schoppert, B. J., and Austin, K. (2007, February 12). *Flexible and adjustable authentication in cyberspace*. USPTO Published Patent Application US2007/0199053, Filing Date: 12 February 2007.

[206] Sandhu, R. S., Schoppert, B. J., Ganesan, R., Bellare, M., and deSa, C. J. (2006a, August 17). *Asymmetric key pair having a kiosk mode*. USPTO Published Patent Application US2006/0182276, Filing Date: 14 February 2005.

[207] Sandhu, R. S., Schoppert, B. J., Ganesan, R., Bellare, M., and deSa, C. J. (2006b, August 17). *Roaming utilizing an asymmetric key pair*. USPTO Published Patent Application US2006/0182277, Filing Date: 14 February 2005.

[208] Sandhu, R. S., Schoppert, B. J., Ganesan, R., Bellare, M., and deSa, C. J. (2006c, August 17). *Architecture for asymmetric crypto-key storage*. USPTO Published Patent Application US2006/0182283, Filing Date: 14 February 2005.

[209] Sandhu, R. S., Schoppert, B. J., Ganesan, R., Bellare, M., and deSa, C. J. (2006d, August 17). *Technique for asymmetric crypto-key generation*. USPTO Published Patent Application US2006/0184786, Filing Date: 14 February 2005.

[210] Sandhu, R. S., Schoppert, B. J., Ganesan, R., Bellare, M., and deSa, C. J. (2006e, August 17). *Authentication protocol using a multi-factor asymmetric key pair*. USPTO Published Patent Application US2006/0184787, Filing Date: 14 February 2005.

[211] Sandhu, R. S., Schoppert, B. J., Ganesan, R., Bellare, M., and deSa, C. J. (2006f, August 17). *Multiple factor private portion of an asymmetric key*. USPTO Published Patent Application US2006/0184788, Filing Date: 14 February 2005.

[212] Sandhu, R. S., Schoppert, B. J., Ganesan, R., Bellare, M., and deSa, C. J. (2007a, March 8). *Technique for providing multiple levels of security*. USPTO Published Patent Application US2007/0055878, Filing Date: 14 February 2005.

[213] Sandhu, R. S., Schoppert, B. J., Ganesan, R., Bellare, M., and deSa, C. J. (2007b, March 22). *Asymmetric crypto-graphy with rolling key security*. USPTO Published Patent Application US2007/0067618, Filing Date: 17 January 2006.

[214] Sandhu, R. S., Schoppert, B. J., Ganesan, R., Bellare, M., and deSa, C. J. (2007c, November 8). *Multifactor split asymmetric crypto-key with persistent key security*. USPTO Published Patent Application US2007/0258585, Filing Date: 5 May 2006.

[215] Sandhu, R. S., Schoppert, B. J., Ganesan, R., Bellare, M., and deSa, C. J. (2007d, November 8). *Secure login using a multifactor split asymmetric crypto-key with persistent key security*. USPTO Published Patent Application US2007/0258594, Filing Date: 5 May 2006.

[216] Scalet, S. D. (2005, December 1). *How to write good passwords*, [Online]. CIO.com. Available: http://www.csoonline.com/article/print/220721 [2008, September 19].

[217] Schneider, J. (2004, December 9). *Graphical event-based password system*. USPTO Published Patent Application US2004/0250138, Filing Date: 18 April 2003.

[218] Schneier, B. (1996). *Applied cryptography: Protocols, algorithms, and code in C* (2nd ed.). New York City, New York, USA: John Wiley & Sons.

[219] Schneier, B. (2006, December 14). *MySpace passwords aren't so dumb*, [Online]. Wired News. Available: http://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300 [2008, June 11].

[220] Schneier, B. (2007, January 11). *Secure passwords keep you safer*, [Online]. Wired News. Available: http://www.wired.com/politics/security/commentary/securitymatters/2007/01/72458 [2008, June 11].

[221] Silverman, J. H. (1986). *The arithmetic of elliptic curve*. New York, NY, USA: Springer-Verlag New York, Inc.

[222] Simmons, G. J. (1984, April 9-11). The subliminal channel and digital signatures. *Proceedings of the Advances in Cryptology (EUROCRYPT '84) (aka Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques 1984)*, LNCS 209, Paris, France, 364-378.

[223] Simmons, G. J. (1998, May). The history of subliminal channels. *IEEE Journal on Selected Areas in Communications, 16*(4), 452-462.

[224] 新加坡女郎患湿疹无指纹纹机场通关检查花 45 分鐘 [Singaporean Female having eczema has no fingerprint spending 45 minutes to get through the airport immigration office]. (2008, August 22-23). *星洲日报* [*Sin Chew Daily*], [Online], p. 17. Available: http://search.sinchew-i.com/node/192066 [2008, September 1].

[225] Spafford, E. H. (1993). *What is a Ph.D. dissertation?*, [Online]. Available: http://spaf.cerias.purdue.edu/~spaf/Archive/spaf.html [2008, August 2].

[226] Stallings, W. (2000). *Network security essentials: Applications and standards*. Upper Saddle River, New Jersey, USA: Prentice Hall.

[227] Stallings, W. (2006). *Cryptography and network security: Principles and practices* (4th ed.). Upper Saddle River, NJ, USA: Pearson Prentice Hall.

[228] Standing, L. (1973, May). Learning 10,000 pictures. *Quarterly Journal of Experimental Psychology, 25*(2), 207-222.

[229] Standing, L., Conezio, J., and Haber, R. (1970). Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. *Psychonomic Science, 19*(2), 73-74.

[230] Suo, X., Zhu, Y., and Owen, G. S. (2005, December 5-9). Graphical passwords: A survey. *Proceedings of the 21st Annual Computer Security Applications Conference 2005 (ACSAC 2005)*, Tucson, Arizona, USA, 463-472.

[231] Swanson, M. D., Kobayashi, M., and Tewfik, A. H. (1998, June). Multimedia data-embedding and watermarking techniques. *Proceedings of the IEEE, 86*(6), 1064-1087.

[232] Tai, C. L. (2001, December 25). *Dual in-line type finger-actuated switch*. USPTO Issued Patent US6333479, Filing Date: 4 January 2001, Issue Date: 25 December 2001.

[233] U.S. Department of Defense. (1985). *Password management guideline* (Report No. CSC-STD-002-85) Fort George G. Meade, Maryland, USA: DoD Computer Center.

[234] Vacca, J. R. (2007, March 16). *Biometric technologies and verification systems*. Oxford, Oxfordshire, UK: Butterworth-Heinemann, p. 280.

[235] Wailgum, T. (2008, September 8). *Password brain teaser: Too many passwords or not enough brain power?*, [Online]. CIO.com. Available: http://www.cio.com/article/print/448241 [2008, September 10].

[236] Wang, X. L. [王学理], and Pei, D, Y. [裴定一]. (2006). *椭圆与超椭圆曲线公钥密码的理论与实现* [Theory and implementation of elliptic curve and hyperelliptic curve cryptography]. Beijing [北京], China [中国]: Science Press [科学出版社]. (in Chinese language).

[237] Weinshall, D., and Kirkpatrick, S. (2004, April 24-29). Passwords you'll never forget, but can't recall. *Proceedings of the Conference on Human Factors in Computing Systems 2004 (CHI 2004)*, Vienna, Austria, 1399-1402.

[238] Wiener, M. J. (1990, May). Cryptanalysis of short RSA secret exponents. *IEEE Transactions on Information Theory, 36*(3), 553-558.

[239] Wikipedia Contributors. (2008a, July 22). *List of languages by number of native speakers*, [Online]. Wikipedia the Free Encyclopedia. Available: http://en.wikipedia.org/w/index.php?title=List_of_languages_by_number_of_native_speakers&oldid=227300820 [2008, July 23].

[240] Wikipedia Contributors. (2008b, August 27). *Writing system*, [Online]. Wikipedia the Free Encyclopedia. Available: http://en.wikipedia.org/w/index.php?title=Writing_system&oldid=234534887 [2008, September 1].

[241] Williams, L. C. (2002). *A discussion of the importance of key length in symmetric and asymmetric cryptography*, [Online]. Bethesda, Maryland, USA: SANS Institute. Available: http://www.giac.org/practical/gsec/Lorraine_Williams_GSEC.pdf [2008, May 17].

[242] Wilson, A. L. (2008, June 11). *Microsoft's CardSpace attacked by researchers*, [Online]. CIO.com. Available: http://www.cio.com/article/print/391813 [2008, September 10].

[243] *Windows Live ID* (aka Microsoft Passport Network), [Online]. (No date). Available: http://www.passport.net [2008, July 16].

[244] Witty, R. J. (2001, January 30). *Best practices for managing PINs and passwords* (Tech. Rep. No. Gartner QA-12-8664). Stamford, CT, USA: Gartner, Inc.

[245] Wolfgang, R. B., Podilchuk, C. I., and Delp, E. J. (1999, July). Perceptual watermarks for digital images and video. *Proceedings of the IEEE, 87*(7), 1108-1126.

[246] Wu, T. J. (2003, March 25). *System and method for securely logging onto a remotely located computer*. USPTO Issued Patent US6539479, Filing Date: 14 July 1998, Issue Date: 25 March 2003.

[247] Yan, J., Blackwell, A., Anderson, R., and Grant, A. (2004, September-October). Password memorability and security: Empirical results. *IEEE Security and Privacy Magazine, 2*(5), 25-31.

[248] Yee, K. P., and Sitaker, K. (2006, July 12-14). Passpet: Convenient password management and phishing protection. *Proceedings of Symposium on Usable, Privacy and Security (SOUPS2006)*, Pittsburgh, PA, USA, 32-43.

[249] Zhu, Y. F. [祝跃飞], and Zhang, Y. J. [张亚娟]. (2006, October). *椭圆曲线公钥密码导引* [Guide to elliptic curve cryptography]. Beijing [北京], China [中国]: Science Press [科学出版社]. (in Chinese language).

ACRONYMS

2D	Two-dimensional
2TDEA	2-Key Triple Data Encryption Algorithm
3TDEA	3-Key Triple Data Encryption Algorithm
2TDES	2-Key Triple Data Encryption Standard
3TDES	3-Key Triple Data Encryption Standard
A-Level	Advanced Level
ACM	Association for Computing Machinery
AD	*anno domini* in Latin language, meaning the Christian era
AES	Advanced Encryption Standard
AIPO/OAPI	African Intellectual Property Organization (Organisation Africaine de la Propriété Intellectuelle)
ANN	Artificial Neural Network
ANN Based BAP	Artificial Neural Network Based Byzantine Agreement Protocol
APA	American Psychological Association
APWG	Anti-Phishing Working Group
ARIPO	African Regional Industrial Property Organization
ASCII	American Standard Code for Information Interchange
AUTM	Association of University Technology Managers
BAP	Byzantine Agreement Protocol
BAP-ANN	Byzantine Agreement Protocol with Artificial Neural Network
BGP	Byzantine Generals Problem
BTIRDM	Budapest Treaty on the International Recognition of the Deposit of Microorganisms for the Purposes of Patent Procedure
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
Cat.	Category
CII	Computer-Implemented Invention
CIS	Cryptography & Information Security
CLJ	Crime, Law, and Justice
CLPP	Chinese Language Passphrase
CLPW	Chinese Language Password
CM	Communication Management
CO	Central Office
CPG	Compass Password Generator
CRPP	Center for Research and Postgraduate Programmes, now called IPS, MMU.
CSPRNG	Cryptographically Secure Pseudo-Random Number Generator
DC	Direct Current

DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DIL / DIP	Dual In-Line Package
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
DSS	Dynamic Security Skins
EAPO	Eurasian Patent Organization
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
EMAIL	Electronic Mail
EPO	European Patent Office
ESP	Extra-Sensory Perception
EU	European Union
FAR	False Acceptance Rate
FCN	Fully Connected Network
FET	Faculty of Engineering & Technology, MMU, Bukit Beruang, Melaka, Malaysia.
FFC	Finite Field Cryptography
FOREX	Foreign Exchange
FRR	False Rejection Rate
FTP	File Transfer Protocol
FTPS	FTP over SSL
GCC	Gulf Cooperation Council
GCCPO	Gulf Cooperation Council Patent Office
GUI	Graphical User Interface
HDD	Hard Disk Drive
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP over SSL
IACR	International Association for Cryptologic Research
IATUL	International Association of Technological University Libraries
IDC	Identity-Based Cryptography
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IEICE	The Institute of Electronics, Information and Communication Engineers （電子情報通信学会）
IETF	Internet Engineering Task Force
IFC	Integer Factorization Cryptography
IIPA	International Intellectual Property Alliance

ILBS	International Law Book Services
IM	Instant Messaging
IMAP4	Internet Message Access Protocol version 4
IP	Intellectual Property
IP	Internet Protocol
IPOS	Intellectual Property Office of Singapore
IPR	Intellectual Property Right
IPS	Institute for Postgraduate Studies, previously called CRPP, MMU.
IRC	Internet Relay Chat
ITRC	Identity Theft Resource Center
JPO	Japan Patent Office （日本経済産業省特許庁）
LCD	Liquid Crystal Display
LPWA	Lucent Personal Web Assistant
LSB	Least Significant Bit
mA	milli-ampere
MAC	Message Authentication Code
MCMC	Malaysian Communications and Multimedia Commission
MDC	Multimedia Development Corporation Sdn Bhd
MDeC	Multimedia Development Corporation Sdn Bhd
MePKC	Memorizable Public-Key Cryptography / Memorizable Public-Key Cryptosystem
MIME	Multipurpose Internet Mail Extensions
MITM	Man In The Middle
MMU	Multimedia University, which is a brand name of UTSB.
mod	modulus
MoPKC	Mobile Public-Key Cryptography
MSB	Most Significant Bit
MSVS	Microsoft Visual Studio
MTSO	Mobile Telephone Switching Office
MY	Malaysia
MyIPO	Intellectual Property Corporation of Malaysia (Perbadanan Harta Intelek Malaysia)
NBER	National Bureau of Economic Research
NIST	National Institute of Standards and Technology
nPDT	n Poles Double Throw
nPST	n Poles Single Throw
OAPI/AIPO	Organisation Africaine de la Propriété Intellectuelle (African Intellectual Property Organization)
OS	Operating System
OSCAR	Open System for CommunicAtion in Realtime (AOL Instant Messenger Protocol for ICQ and AIM)

OTP	One-Time Password
P-192	192-bit Pseudo-Random Curve over Prime Field of ECC
PAKE	Password-Authenitcated Key Exchange
PC	Personal Computer
PCB	Printed Circuit Board
PCPIP	Paris Convention for the Protection of Industrial Property
PCT	Patent Cooperation Treaty
PGP	Pretty Good Privacy
Ph.D.	Doctor of Philosophy
PKC	Public-Key Cryptography
PKC	Public-Key Cryptosystem
PLT	Patent Law Treaty
PNAS	Proceedings of the National Academy of Sciences
POP3	Post Office Protocol version 3
P.R.C.	People's Republic of China （中华人民共和国）
PRNG	Pseudo-Random Number Generator
PSTN	Public Switched Telephone Network
RFC	Request for Comments
RFID	Radio Frequency Identification
Rlogin	Remote Login in UNIX Systems
RNG	Random Number Generator
R.O.C.	Republic of China （中華民國）
RSA	Rivest-Shamir-Adleman Public-Key Cryptography
S/MIME	Secure / Multipurpose Internet Mail Extensions
SATA	Serial Advanced Technology Attachment
SD	Statutory Declaration
Sdn. Bhd.	"Sendirian Berhad" in Malayan language, i.e. private limited in English language.
SFTP	Secure FTP over SSH
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SIPO	State Intellectual Property of the P.R.C. （中华人民共和国国家知识产权局）
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SPC	Strasbourg Patent Convention
SPEKE	Simple Password Exponential Key Exchange
SPLT	Substantive Patent Law Treaty

SP1	Service Pack 1
SP2	Service Pack 2
SP3	Service Pack 3
SPP	Single Password Protocol
SRP	Secure Remote Password Protocol
SRP-6	Secure Remote Password Protocol version 6
SSH	Secure Shell
SSL	Secure Sockets Layer
STPM	Sijil Tinggi Persekolahan Malaysia (in Malayan language), Malaysia Higher School Certificate (in English language)
TAC	Transaction Authorisation Code or Transaction Authentication Code
TAP	Transaction Authorization Pin
TELNET	Telecommunication Network
TIPO	The Intellectual Property Office of Ministry of Economic Affairs, R.O.C. （中華民國經濟部智慧財產局）
TLS	Transport Layer Security
TRIPS	Agreement on Trade Related Aspects of Intellectual Property Rights
TSIG	Transaction SIGnature Protocol
TSA	Timestamping Authority
TSP	Time-Stamp Protocol
TTP	Trusted Third Party
UI	Utility Innovation
UK	United Kingdom
UKCS	UK Copyright Service
UN	United Nations
UNESCOBKK	UNESCO Bangkok
UNODC	United Nations Office on Drugs and Crime
US	United States
USA	United States of America
USB	Universal Serial Bus
USCO	US Copyright Office
USCOC	US Chamber of Commerce
USPTO	US Patent and Trademark Office
UTSB	Universiti Telekom Sdn. Bhd., Malaysia.
V	Volt
WIPO	World Intellectual Property Organization
WM	Watermarking
WTO	World Trade Organization

PUBLICATION LIST BY K.-W. LEE

[1] Lee, K. W. (2008a, May 8). *An improved dual in-line (DIL) switch for securing data communication and storage*. Malaysia Application of Utility Innovation (aka utility model or small patent) UI 20070733, MyIPO, Filing Date: 11 May 2007, Grant Date: 30 June 2010, Patent No.: MY-141830-A.

[2] Lee, K. W. (2008b, May 8). *An improved dual in-line (DIL) switch for securing data communication and storage*. PCT Patent Application PCT/MY2008/000040, WIPO, Filing Date: 8 May 2008, Publication Date: 20 November 2008.

[3] Lee, K. W. [李國華]. (2008c, May 9). *應用於保護資料通訊及存儲安全之改良式雙行開關* [An improved dual in-line (DIL) switch for securing data communication and storage]. Taiwan (ROC) Patent Application TW097117364, TIPO, Filing Date: 9 May 2008. (in Chinese language).

[4] Lee, K. W. (2008h, July 25). *Methods and systems to create big memorizable secrets and their applications in information engineering*. Malaysia Patent Application PI 20082771, MyIPO, Filing Date: 25 July 2008.

[5] Lee, K. W. (2008k, December 10). *Methods and systems to create big memorizable secrets and their applications in information engineering*. Singapore Patent Application SG 200809162-1, IPOS, Filing Date: 10 December 2008, Now Abandoned.

[6] Lee, K. W. (2008l, December 18). *Methods and systems to create big memorizable secrets and their applications in information engineering*. PCT Patent Application PCT/IB2008/055432, WIPO, Filing Date: 18 December 2008, Publication Date: 28 January 2010.

[7] Lee, K. W. (2009b, April). High-Entropy 2-Dimensional Key Input Method for Symmetric and Asymmetric Key Cryptosystems. *International Journal of Computer and Electrical Engineering (IJCEE), 1*(1), 1-8.

[8] Lee, K. W. (2010b, September 15). *Methods and systems to create big memorizable secrets and their applications in information engineering*. Singapore Patent Application SG 200809162-1, IPOS, Filing Date: 15 September 2010.

[9] Lee, K. W. (2010c, November 08). *Methods and systems to create big memorizable secrets and their applications in information engineering*. United States Patent Application US 2011/0055585, USPTO, Filing Date (Completion): 08 November 2010.

[10] Lee, K. W., and Ewe, H. T. (2006, November 3-6). Coinware for multilingual passphrase generation and its application for Chinese language password. *Proceedings of the 2006 International Conference on Computational Intelligence and Security (CIS 2006)*, Guangzhou, Guangdong, China, 1511-1514 (Part 2).

[11] Lee, K. W., and Ewe, H. T. (2007, August). Multiple hashes of single key with passcode for multiple accounts. *Journal of Zhejiang University Science A (JZUS-A), 8*(8), 1183-1190.